Stellungnahme 28/2018

zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission

über die Angemessenheit des Schutzes personenbezogener Daten in Japan

Angenommen am 5. Dezember 2018

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 70 Absatz 1 Buchstabe s der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „DSGVO“),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung vom 25. Mai 2018 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG

1. Die Europäische Kommission billigte ihren Entwurf eines Durchführungsbeschlusses über die Angemessenheit des Schutzes personenbezogener Daten durch Japan gemäß der Datenschutz-Grundverordnung (nachstehend: DSGVO)[1] am 5. September 2018.[2] Daraufhin leitete die Europäische Kommission das Verfahren für seine förmliche Annahme ein.

2. Am 25. September 2018 ersuchte die Europäische Kommission den Europäischen Datenschutzausschuss („EDSA“) um eine Stellungnahme.[3] Die Kommission wurde aufgefordert, dem EDSA alle erforderlichen Unterlagen über dieses Land zu übermitteln, einschließlich aller einschlägigen Korrespondenz mit der japanischen Regierung.

3. Im Lichte der Diskussionen mit dem EDSA nahm die Europäische Kommission zweimal Änderungen an ihrem Entwurf des Angemessenheitsbeschlusses vor und übermittelte ihre letzte Fassung am 13. November 2018.[4] Der EDSA legt seine vorliegende Stellungnahme auf der Grundlage dieser neuesten Fassung des Entwurfs eines Durchführungsbeschlusses (im Folgenden „Entwurf des Angemessenheitsbeschlusses“) vor.

4. Der EDSA stützte seine Bewertung des durch den Angemessenheitsbeschluss der Kommission gewährleisteten Schutzniveaus auf eine Prüfung des Beschlusses selbst sowie auf die Grundlage einer Auswertung der von der Kommission[5] bereitgestellten Unterlagen[6].

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
[2] Siehe Pressemitteilung http://europa.eu/rapid/press-release_IP-18-5433_de.htm.
[3] Gemäß Artikel 70 Absatz 1 Buchstabe s DSGVO.
[4] Siehe Anhang I der Stellungnahme des EDSA für die aktualisierte Fassung des Entwurfs eines Durchführungsbeschlusses der Europäischen Kommission.
[5] Siehe Anhang II der Stellungnahme des EDSA für das Verzeichnis von Unterlagen, die dem EDSA nicht von der Europäischen Kommission bereitgestellt wurden.
[6] Der EDSA stützte sich in seiner Analyse auf Übersetzungen, die von den japanischen Behörden vorgelegt und von der Europäischen Kommission überprüft wurden.

5. In den Mittelpunkt seiner Bewertung stellte der EDSA sowohl die kommerziellen Aspekte des Entwurfs des Angemessenheitsbeschlusses als auch den Zugang der Regierung zu personenbezogenen Daten, die aus der EU zum Zwecke der Strafverfolgung und der nationalen Sicherheit übermittelt werden, einschließlich der Rechtsmittel, die EU-Bürgern zur Verfügung stehen. Der EDSA prüfte auch, ob die im japanischen Rechtsrahmen vorgesehenen Garantien tatsächlich vorhanden und wirksam sind.

6. Als Hauptbezugspunkt für diese Arbeit hat der EDSA sein im Februar 2018 angenommenes Referenzpapier zur Angemessenheit[7] verwendet.

1.1 Konvergenzbereiche

7. Das wichtigste Ziel des EDSA bestand darin, der Europäischen Kommission eine Stellungnahme zum Schutzniveau für natürliche Personen innerhalb des japanischen Rechtsrahmens an die Hand zu geben. Natürlich erwartet der EDSA nicht, dass der japanische Rechtsrahmen eine Kopie des europäischen Datenschutzrechts ist.

8. Der EDSA weist jedoch darauf hin, dass die Rechtsprechung des EuGH und Artikel 45 DSGVO verlangen, dass die Rechtsvorschriften des Drittlandes an den Kern der in der DSGVO verankerten Grundsätze angeglichen sein müssen, damit davon ausgegangen werden kann, dass sie ein angemessenes Schutzniveau bieten. Im Bereich Datenschutz stellt der EDSA ferner fest, dass es Schlüsselbereiche der Angleichung zwischen dem Rahmen der DSGVO und dem japanischen Rechtsrahmen in Bezug auf bestimmte Kernbestimmungen gibt, wie Richtigkeit von Daten und Datenminimierung, Beschränkung der Speicherung, Datensicherheit, Zweckbindung und eine unabhängige Aufsichtsbehörde, die Kommission für den Schutz personenbezogener Daten (PPC).

9. Darüber hinaus begrüßt der EDSA die Bemühungen der Europäischen Kommission und der japanischen Behörden, dafür zu sorgen, dass Japan ein der DSGVO angemessenes Schutzniveau bietet, insbesondere durch ein Schließen der Lücken zwischen der DSGVO und dem japanischen Datenschutzrahmen durch die Annahme zusätzlicher Vorschriften durch die PPC, die nur für personenbezogene Daten gelten, die aus der EU nach Japan übermittelt werden („die Ergänzenden Vorschriften“). So hält der EDSA beispielsweise fest, dass die PPC sich bereit erklärt hat, weitere Datenkategorien als sensible Daten zu behandeln (sensible Daten nach japanischem Recht umfassen weder Daten zur sexuellen Orientierung noch zur Mitgliedschaft in einer Gewerkschaft). Darüber hinaus wird durch die Ergänzenden Vorschriften sichergestellt, dass die Rechte der betroffenen Person für alle aus der EU übermittelten personenbezogenen Daten unabhängig von ihrer Speicherfrist gelten (wohingegen das japanische Rechtssystem vorsieht, dass die Rechte der betroffenen Person nicht für personenbezogene Daten gelten, deren Löschung innerhalb eines Zeitraums von sechs Monaten vorgesehen ist).

10. Der EDSA nimmt ferner die Bemühungen der Europäischen Kommission zur Kenntnis, den Angemessenheitsbeschluss durch das Eingehen auf die Bedenken des EDSA noch zu verbessern.

1.2 Allgemeine Herausforderungen

11. Dennoch gibt es nach wie vor Herausforderungen, und der EDSA schlägt folgende Schwerpunktbereiche vor, die im japanischen System gestärkt und genau überwacht werden sollten.

12. Die erste Herausforderung besteht in der Überwachung dieser neuen Angemessenheitsarchitektur, die eine Kombination aus bestehendem Rechtsrahmen und spezifischen Ergänzenden Vorschriften ist und sicherstellen soll, dass es ein nachhaltiges und zuverlässiges System geben wird, das keine **praktischen**

[7] WP254, Referenzpapier zur Angemessenheit, 6. Februar 2018.

Probleme bei der konkreten und wirksamen Einhaltung der Vorschriften durch japanische Unternehmen und bei der Durchsetzung durch die PPC hervorruft.

13. Zweitens nimmt der Europäische Datenschutzausschuss die wiederholten Zusagen und Zusicherungen der Europäischen Kommission und der japanischen Behörden in Bezug auf den verbindlichen und durchsetzbaren Charakter der Ergänzenden Vorschriften zur Kenntnis, fordert die Kommission jedoch auf, **ihre Verbindlichkeit und ihre effektive Anwendung in Japan kontinuierlich zu überwachen**, da ihr rechtlicher Wert ein absolut wesentliches Element der Angemessenheit EU - Japan ist. Bezüglich der Leitlinien der PPC würde der EDSA Präzisierungen im Entwurf des Angemessenheitsbeschlusses im Hinblick auf **deren Verbindlichkeit** begrüßen **und fordert die Kommission auf, diesen Aspekt aufmerksam zu überwachen**.[8]

1.3 Besondere kommerzielle Aspekte

14. Im Bereich der kommerziellen Aspekte des Entwurfs eines Angemessenheitsbeschlusses zwischen der EU und Japan hat der EDSA einige spezifische Bedenken und fordert Präzisierungen zu einigen wichtigen Fragen.

1.3.1 Bedenken des EDSA im Hinblick auf wichtige Datenschutzgrundsätze

15. Der EDSA begrüßt, dass die Ergänzenden Vorschriften ausschließen, dass personenbezogene Daten, die aus der EU übermittelt werden, auf der Grundlage von APEC – CBPR an ein Drittland weiterübermittelt werden. Darüber hinaus erkennt der EDSA an, dass sich die Europäische Kommission in ihrem neuen Entwurf des Angemessenheitsbeschlusses dazu verpflichtet hat, den Angemessenheitsbeschluss auszusetzen, wenn Weiterübermittlungen nicht länger die Kontinuität des Schutzes gewährleisten würden.

16. Nach japanischem Recht ist eine der Rechtsgrundlagen für die Weiterübermittlung die Anerkennung eines Drittlandes als Land, das ein dem japanischen Level angemessenes Schutzniveau bietet. Die Einschätzung eines Drittlandes durch Japan als Land mit angemessenem Schutzniveau scheint jedoch nicht die zwischen der Europäischen Kommission und der PPC ausgehandelten spezifischen „Ergänzenden Vorschriften“ zu umfassen, die nur für personenbezogene Daten aus der EU gelten und ein Schutzniveau gewährleisten sollen, das in der Sache den Standards der DSGVO gleichwertig ist. Daraus folgt, dass personenbezogene Daten aus der EU, die von Japan auf der Grundlage eines japanischen Angemessenheitsbeschlusses in ein anderes Drittland übermittelt werden, das nicht als über einen mit der DSGVO gleichwertigen Datenschutzrahmen verfügend gilt, dann nicht zwangsläufig auch weiterhin den spezifischen Schutz von personenbezogenen Daten aus der EU genießen.

17. **Es sollte jedoch berücksichtigt werden, dass Weiterübermittlungen personenbezogener Daten an Drittländer erfolgen können, die möglicherweise später Gegenstand eines japanischen Angemessenheitsbeschlusses werden. Diese Drittländer sind möglicherweise zuvor keiner Bewertung oder Feststellung der Angemessenheit durch die EU unterzogen worden. An diesem Punkt sollte die Kommission überwachend tätig werden und sicherstellen, dass das Schutzniveau für EU-Daten aufrechterhalten wird, oder eine Aussetzung dieses Angemessenheitsbeschlusses in Betracht ziehen.**

18. Darüber hinaus hat der EDSA Bedenken beim Thema **Einwilligung** und bei den **Transparenzpflichten** von für die Verarbeitung Verantwortlichen (PIHBO). Der EDSA hat diese Aspekte sorgfältig geprüft, weil anders als im europäischen Datenschutzrecht die Einwilligung als Grundlage für die Verarbeitung und für Übermittlungen in der japanischen Rechtsordnung eine zentrale Rolle spielt. So hat der EDSA

[8] Für weitere Informationen siehe Abschnitt 1.3.4 dieser Stellungnahme.

beispielsweise Bedenken in Bezug auf den Begriff der Einwilligung, dessen Definition nicht das Recht auf Widerruf der Einwilligung umfasst, ein wesentliches Element des EU-Rechts, mit dem sichergestellt werden soll, dass die betroffene Person eine echte Kontrolle über ihre personenbezogenen Daten ausübt. Hinsichtlich der Transparenzpflichten eines PIHBO bestehen Zweifel, ob betroffene Personen proaktiv informiert werden.

19. Der EDSA ist besorgt darüber, dass das **japanische Rechtsbehelfssystem** für Personen in der EU möglicherweise nicht leicht zugänglich ist, wenn sie Unterstützung benötigen oder eine Beschwerde einreichen möchten, da die Unterstützung durch die PPC nur über eine Helpline und nur in japanischer Sprache erhältlich ist. Dasselbe Problem besteht bei Mediationsdiensten, die von der PPC angeboten werden, da das System nicht auf der englischen Fassung der PPC-Website veröffentlicht wird, während wichtige Informationsunterlagen, wie häufig gestellte Fragen zum APPI, auch nur auf Japanisch zur Verfügung stehen. Diesbezüglich würde es der EDSA begrüßen, wenn die Kommission mit der PPC die Möglichkeit erörtern könnte, zumindest in englischer Sprache einen Online-Dienst einzurichten, über den Personen in der EU Unterstützung erhalten und Beschwerden einreichen können, ähnlich wie der in Anhang II dieses Angemessenheitsbeschlusses vorgesehene. Die Europäische Kommission wird auch die Wirksamkeit von Sanktionen und entsprechenden Abhilfemaßnahmen genau überwachen müssen.

1.3.2 Klarstellungsbedarf

20. Der EDSA würde Zusicherungen zu einigen Aspekten des Entwurfs des Angemessenheitsbeschlusses begrüßen, zu denen noch weitere Präzisierungen erforderlich sind.

21. Dies betrifft beispielsweise einige Schlüsselbegriffe des japanischen Rechts. An Klarheit fehlt es insbesondere in Bezug auf den **Status des so genannten „Treuhänders“** – eine Bezeichnung, die der des Auftragsverarbeiters in der DSGVO ähnelt, aber dessen Fähigkeit, die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu bestimmen und zu ändern, unklar bleibt.

22. Ferner benötigt der EDSA aufgrund fehlender aussagekräftiger Dokumente Zusicherungen zu der Frage, ob die **Einschränkungen der Rechte des Einzelnen** (insbesondere das Recht auf Auskunft, Berichtigung und Widerspruch) in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind und den Wesensgehalt der Grundrechte achten.

23. Der EDSA erwartet außerdem, dass die Europäische Kommission den wirksamen Schutz **personenbezogener Daten, die auf der Grundlage des Entwurfs des Angemessenheitsbeschlusses aus der EU nach Japan übermittelt werden**, **während ihres gesamten „Lebenszyklus“** genau überwacht, auch wenn die japanischen Rechtsvorschriften eine Aufzeichnungspflicht hinsichtlich des Ursprungs der Daten für einen Zeitraum von höchstens drei Jahren vorsehen.

1.4 Über den Zugang von Behörden zu nach Japan übermittelten Daten

24. Der EDSA hat auch den Rechtsrahmen für japanische Regierungsstellen geprüft, innerhalb dessen sie Zugang zu personenbezogenen Daten haben, die für Zwecke der Strafverfolgung oder der nationalen Sicherheit aus der EU nach Japan übermittelt werden. Unter Berücksichtigung der Zusicherungen der japanischen Regierung, die als Anhang II des Entwurfs des Angemessenheitsbeschlusses bezeichnet werden, hat der EDSA eine Reihe von Aspekten ermittelt, die der Klarstellung bedürfen bzw. Anlass zu Bedenken geben, und von denen auf folgende näher eingegangen werden soll.

25. Im Bereich der Strafverfolgung hält der EDSA fest, dass die Rechtsgrundsätze, die für den Zugang zu Daten gelten, häufig mit den Vorschriften in der EU vergleichbar zu sein scheinen, soweit sie verfügbar sind. Das Fehlen von Übersetzungen verschiedener Rechtstexte und der einschlägigen Rechtsprechung macht es jedoch schwierig, zu dem Schluss zu kommen, dass alle Verfahren für den Zugang zu Daten

notwendig und verhältnismäßig sind und dass die Anwendung dieser Grundsätze auf eine Art und Weise erfolgt, die dem EU-Recht „im Wesentlichen gleichwertig“ ist.

26. Im Bereich der nationalen Sicherheit erkennt der EDSA an, dass die japanische Regierung bekräftigt hat, dass Informationen nur aus frei zugänglichen Quellen oder durch freiwillige Offenlegung durch Unternehmen gewonnen werden können und dass sie keine Informationen über die breite Öffentlichkeit sammelt. Er ist sich jedoch der von Sachverständigen und Medien geäußerten Bedenken bewusst und würde eine weitere Klärung der Überwachungsmaßnahmen durch japanische Regierungsstellen begrüßen.

27. Was Rechtsbehelfe für EU-Bürger betrifft, so begrüßt der EDSA, dass die Europäische Kommission und die japanische Regierung einen zusätzlichen Mechanismus für EU-Bürger ausgehandelt haben, um ihnen zusätzliche Rechtsbehelfsmöglichkeiten zur Verfügung zu stellen und damit die Befugnisse der japanischen Datenschutzbehörde auszuweiten. Problematisch ist jedoch nach wie vor, dass dieser neue Mechanismus die Unzulänglichkeiten im Bereich der Aufsicht und der Rechtsbehelfe nach japanischem Recht nicht vollständig kompensiert. Der EDSA strebt daher weitere Präzisierungen an, um sicherzustellen, dass dieser neue Mechanismus diese Mängel vollständig ausgleicht.

1.5 Schlussfolgerung

28. Nach Auffassung des EDSA ist dieser Angemessenheitsbeschluss von allergrößter Bedeutung. Der erste Angemessenheitsbeschluss seit Inkrafttreten der DSGVO wird **ein Präzedenzfall für künftige Anträge auf Prüfung der Angemessenheit sowie für die Überprüfung der nach der Richtlinie 95/46[9] angenommenen Angemessenheitsbeschlüsse** sein. Es sei ferner betont, dass sich die Bürger der Auswirkungen der Globalisierung auf ihre Privatsphäre immer stärker bewusst werden und bei ihren Aufsichtsbehörden darauf drängen, dass angemessene Garantien bestehen, wenn ihre personenbezogenen Daten ins Ausland übermittelt werden. Angesichts dieser Implikationen sollte die Europäische Kommission nach Ansicht des EDSA sicherstellen, dass der durch die Angemessenheit EU - Japan gebotene Schutz nicht beeinträchtigt wird und dass diese spezifische Art der Angemessenheit mit den Anforderungen von Artikel 45 DSGVO in Einklang steht.

29. Der EDSA begrüßt die Bemühungen der Europäischen Kommission und der japanischen PPC, den japanischen Rechtsrahmen so weit wie möglich an den europäischen Rechtsrahmen anzugleichen. Die durch die Ergänzenden Vorschriften bewirkten **Verbesserungen** zur Überbrückung einiger der Unterschiede zwischen den beiden Regelwerken sind sehr wichtig und begrüßenswert.

30. Nach sorgfältiger Prüfung des Entwurfs des Angemessenheitsbeschlusses der Kommission sowie des japanischen Datenschutzrahmens stellt der EDSA jedoch fest, dass weiterhin **eine Reihe von Bedenken sowie Bedarf an weiteren Präzisierungen bestehen**. Darüber hinaus wirft diese spezifische Art der Angemessenheit, die einen bestehenden nationalen Rechtsrahmen mit zusätzlichen spezifischen Vorschriften kombiniert, auch Fragen hinsichtlich ihrer operativen Umsetzung auf. Vor diesem Hintergrund empfiehlt der EDSA der Europäischen Kommission, sich mit den Bedenken und Klarstellungsersuchen des EDSA zu befassen und weitere Belege und Erläuterungen zu den aufgeworfenen Fragen vorzulegen. Der EDSA fordert die Europäische Kommission ferner auf, eine Überprüfung dieser Angemessenheitsfeststellung (mindestens) alle zwei Jahre und nicht alle vier Jahre vorzunehmen, wie im vorliegenden Entwurf des Angemessenheitsbeschlusses vorgeschlagen.

[9] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

2 EINLEITUNG

2.1 Japans Datenschutzrahmen

31. Japans Datenschutzrahmen wurde erst kürzlich, nämlich 2017, modernisiert. Dieser Rahmen stützt sich auf mehrere Pfeiler, in deren Mittelpunkt ein allgemeines Gesetz steht, das Gesetz über den Schutz personenbezogener Daten (APPI). Eine weitere wichtige Rechtsvorschrift ist die Kabinettsverordnung zur Umsetzung des APPI („Kabinettsverordnung"), in der bestimmte Kernprinzipien des APPI festgelegt sind.

32. Auf der Grundlage eines Kabinettsbeschlusses vom 12. Juni 2018[10] wurde mit Artikel 6 des APPI der PPC die Befugnis erteilt, „*die notwendigen Maßnahmen zu treffen, um die Unterschiede zwischen den Systemen und Verfahren zwischen Japan und dem betreffenden Land zu überbrücken und so einen angemessenen Umgang mit den von den einzelnen Ländern erhaltenen personenbezogenen Daten zu gewährleisten*".[11] Der Kabinettsbeschluss regt ferner an, dass die von der PPC erlassenen Regelungen, die die Bestimmungen des APPI ergänzen oder darüber hinausgehen, für japanische Unternehmen verbindlich und durchsetzbar sein sollen.[12]

33. Dementsprechend nahm die PPC Verhandlungen mit der Europäischen Kommission auf und verabschiedete im Juni 2018 strengere Regeln als die des APPI und der Kabinettsverordnung, die auf die aus der EU übermittelten Daten anzuwenden sind. Dabei handelt es sich um die Ergänzenden Vorschriften im Rahmen des Gesetzes über den Schutz personenbezogener Daten, die auf den Umgang mit auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelten Daten anzuwenden sind (im Folgenden „Ergänzende Vorschriften").[13] Diese Ergänzenden Vorschriften sind auch dem im Juli 2018 veröffentlichten Entwurf des Durchführungsbeschlusses der Kommission beigefügt.

34. Es sei darauf hingewiesen, dass die Ergänzenden Vorschriften nur auf personenbezogene Daten anzuwenden sind, die auf der Grundlage des Angemessenheitsbeschlusses aus der Europäischen Union nach Japan übermittelt werden, und darauf abzielen, den Schutz dieser Daten zu verstärken. Sie gelten nicht für personenbezogene Daten von Personen in Japan oder für Daten aus anderen Ländern als denen des EWR.

35. Darüber hinaus weist der EDSA darauf hin, dass das geänderte APPI am 30. Mai 2017 in Kraft trat und die PPC in ihrer derzeitigen Form 2016 eingesetzt wurde. Darüber hinaus müssen die von der PPC mit der Europäischen Kommission ausgehandelten Ergänzenden Vorschriften noch in Kraft treten; dies wird von der Anerkennung Japans als eine Rechtsordnung abhängen, die von der Europäischen Kommission als der in der EU vorhandenen angemessen eingestuft wird.

2.2 Umfang der Bewertung durch den EDSA

36. Der Entwurf des Angemessenheitsbeschlusses der Europäischen Kommission ist das Ergebnis einer Bewertung der japanischen Datenschutzbestimmungen, gefolgt von Verhandlungen mit den japanischen Behörden. Die Ergebnisse dieser Verhandlungen sind vor allem in die beiden Anhänge des

[10] Der EDSA hält fest, dass gemäß dem Entwurf des Angemessenheitsbeschlusses dieser Kabinettsbeschluss am 12. Juni 2018 angenommen wurde. Allerdings erhielt der EDSA lediglich den Entwurf des Kabinettsbeschlusses vom April 2018.

[11] Kabinettsbeschluss vom 25. April 2018.

[12] Siehe weiter unten Abschnitt 1.3.4 für nähere Informationen.

[13] Ergänzende Vorschriften, Anhang I des Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan, dem EDSA im September 2018 übermittelt.

Entwurfs des Angemessenheitsbeschlusses eingegangen: Der erste sieht zusätzliche Schutzmechanismen vor, die japanische Unternehmen bei der Verarbeitung personenbezogener Daten aus der EU anwenden müssen, während der zweite Zusicherungen und Zusagen der japanischen Regierung in Bezug auf den Zugang von Behörden zu Daten enthält.

37. Der EDSA hat den japanischen Datenschutzrahmen, die von der Europäischen Kommission ausgehandelten Ergänzenden Vorschriften sowie die Zusicherungen und Zusagen der japanischen Regierung geprüft. Es wird vom EDSA erwartet, dass er eine unabhängige Stellungnahme zu den Feststellungen der Europäischen Kommission abgibt, gegebenenfalls Unzulänglichkeiten im Angemessenheitsrahmen feststellt und versucht, Änderungen vorzuschlagen, um diese zu beheben.

38. Wie es in dem Referenzpapier zur Angemessenheit des EDSA heißt, sollten *„die von der Kommission bereitgestellten Informationen umfassend sein und es dem EDSA ermöglichen, das Datenschutzniveau im betreffenden Drittland selbst zu beurteilen".*[14]

39. Dessen ungeachtet erhielt der EDSA die meisten Dokumente in englischer Übersetzung, auf die im Entwurf des Angemessenheitsbeschlusses Bezug genommen wird und die wesentlicher Bestandteil des japanischen Rechtssystems sind. Der EDSA gibt daher die vorliegende Stellungnahme auf der Grundlage der Auswertung der in englischer Sprache vorliegenden Dokumente ab. Berücksichtigt hat der EDSA den geltenden Datenschutzrahmen in der Europäischen Union, einschließlich Artikel 8 der Europäischen Menschenrechtskonvention (im Folgenden: („EMRK") zum Schutz des Rechts auf Achtung des Privat- und Familienlebens sowie die Artikel 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (im Folgenden „die Charta") über die Achtung des Privat- und Familienlebens, den Schutz personenbezogener Daten bzw. das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht. Darüber hinaus hat der EDSA den Anforderungen der DSGVO Rechnung getragen und sich mit der einschlägigen Rechtsprechung befasst.

40. Auf diese Weise soll sichergestellt werden, dass der japanische Datenschutzrahmen in der Sache dem der Europäischen Union gleichwertig ist. Das Konzept des „angemessenen Schutzniveaus", das bereits in der Richtlinie 95/46 existierte, wurde vom EuGH weiterentwickelt. Es ist wichtig, auf den vom EuGH in der Rechtssache *Schrems* festgelegten Standard hinzuweisen, nämlich dass das „Schutzniveau" in dem Drittland zwar „dem in der Union garantierten Niveau im Wesentlichen gleichwertig sein muss" – dass sich aber „die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden".[15] Es geht daher nicht darum, in jedem einzelnen Punkt ein Spiegel der europäischen Gesetzgebung zu sein, sondern die grundlegenden und zentralen Anforderungen der zu prüfenden Rechtsvorschriften festzustellen. Angemessenheit kann durch eine Kombination von gegenüber den Betroffenen eingeräumten Rechten, bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden, und die Aufsicht durch unabhängige Behörden erreicht werden. Datenschutzvorschriften sind allerdings nur dann wirksam, wenn sie durchsetzbar sind und in der Praxis eingehalten werden. Daher sind nicht nur der Inhalt der geltenden Vorschriften für die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation zu beachten, sondern auch das System, mit dem die Wirksamkeit der Regeln gesichert werden soll. Effiziente Durchsetzungsmechanismen sind für die Wirksamkeit der Datenschutzvorschriften von wesentlicher Bedeutung.[16]

[14] WP254, S. 4.
[15] Rechtssache C-362/14, Maximillian Schrems / Data Protection Commissioner, 6. Oktober 2015 (Rn. 73, 74).
[16] WP254, S. 3.

2.3 Allgemeine Bemerkungen und Bedenken

2.3.1 Besonderheiten dieser Art von Angemessenheitsbeschluss

41. Die Angemessenheit EU - Japan ist der erste Fall, der vor dem neuen rechtlichen Hintergrund der DSGVO geprüft wird. Dies verleiht der Arbeit des EDSA angesichts der Auswirkungen dieses Entwurfs für einen Angemessenheitsbeschluss auf künftige Anträge auf Prüfung der Angemessenheit eine umso größere Bedeutung.

42. Die Angemessenheit EU - Japan wäre auch der erste auf Gegenseitigkeit beruhende Fall. Wenn die EU anerkennt, dass Japan ein im Wesentlichen der DSGVO gleichwertiges Schutzniveau bietet, wird Japan seinen eigenen Angemessenheitsbeschluss nach Artikel 24 des APPI vorlegen, in dem anerkannt wird, dass die EU ein Datenschutzniveau bietet, das dem des japanischen Datenschutzrahmens angemessen ist. Daher ist die in Aussicht genommene Angemessenheit Japan – EU von einer besonderen Art, die der EDSA bei seiner Bewertung berücksichtigt hat. Wie bereits erwähnt, hat die japanische PPC spezifische, strengere Vorschriften mit der Europäischen Kommission ausgehandelt, die nur für aus der EU übermittelte personenbezogene Daten gelten. Diese strengeren Vorschriften sind nach dem Kabinettsbeschluss verbindlich und durchsetzbar und müssen bei der Verarbeitung personenbezogener Daten aus der EU, die nach dem vorliegenden Entwurf eines Angemessenheitsbeschlusses erfolgt, von allen Personal Information Handling Business Operators (im Folgenden „PIHBO“) in Japan eingehalten werden.

43. Die Europäische Kommission hat daher ihre Angemessenheitsfeststellung nicht nur auf den bestehenden allgemeinen japanischen Datenschutzrahmen, sondern auch auf diese spezifischen Vorschriften gestützt. Die Tatsache, dass Ergänzende Vorschriften das APPI begleiten sollen, ist ein Hinweis darauf, dass die Europäische Kommission einräumt, dass die japanischen Datenschutzvorschriften nicht *per se* der DSGVO im Wesentlichen gleichwertig sind.

44. **In Anbetracht der erwähnten Probleme fordert der EDSA die Europäische Kommission auf, dafür Sorge zu tragen, dass diese neue Angemessenheitsarchitektur, die erste, die vor dem Hintergrund der DSGVO angenommen wird und sich auf Ergänzende Vorschriften stützt, ein nachhaltiges und zuverlässiges System ist, das bei der konkreten und effizienten Einhaltung der Vorschriften durch japanische Unternehmen und bei der Durchsetzung durch die PPC keine praktischen Fragen aufwirft.**

2.3.2 Zuverlässigkeit der Übersetzungen

45. Wie die Europäische Kommission hat auch der EDSA auf der Grundlage der von den japanischen Behörden bereitgestellten englischen Übersetzungen gearbeitet.[17] Der EDSA fordert die Europäische Kommission auf, klarzustellen, dass sie ihren Entwurf des Angemessenheitsbeschlusses auf die erhaltenen englischen Übersetzungen gestützt hat, und die Qualität und Zuverlässigkeit dieser Übersetzungen regelmäßig zu überprüfen.

2.3.3 Sektorale Angemessenheit

46. Die Feststellung der Angemessenheit dieses Entwurfs für eine Angemessenheitsentscheidung beschränkt sich auf den Schutz personenbezogener Daten durch PIHBO im Sinne des APPI. Dies bedeutet, dass die Angemessenheit sektorspezifisch ist, da sie nur für den privaten Sektor gilt, nicht aber für die Übermittlung personenbezogener Daten zwischen Behörden und öffentlichen Stellen. Derzeit erwähnt die Europäische Kommission kurz diese Besonderheit des Anwendungsbereichs der Angemessenheit in Erwägungsgrund 10 des Entwurfs des Angemessenheitsbeschlusses.

[17] Die Europäische Kommission hat diese Übersetzungen überprüft.

47. **Der EDSA fordert die Europäische Kommission auf, im Einklang mit Artikel 45 Absatz 3 DSGVO ausdrücklich auf den sektoralen Charakter dieser Angemessenheitsfeststellung im Titel des Durchführungsbeschlusses sowie in dessen Artikel 1 hinzuweisen.**

2.3.4 Verbindlichkeit der Ergänzenden Vorschriften und von Leitlinien der PPC

48. In Artikel 6 des APPI heißt es: „Die Regierung erlässt die erforderlichen gesetzgeberischen und sonstigen Maßnahmen, um diskret personenbezogene Informationen schützen zu können, die eine strikte Anwendung der Vorschriften erfordern, damit die Rechte und Interessen von Einzelpersonen besser geschützt werden, und sie ergreift in Zusammenarbeit mit den Regierungen anderer Länder die erforderlichen Maßnahmen, um durch die Förderung der Zusammenarbeit mit einer internationalen Organisation und einem anderen internationalen Rahmen ein international konformes System für personenbezogene Daten zu errichten." Zwar wird in diesem Artikel des APPI die Regierung eindeutig als für solche rechtlichen Schritte zuständig bezeichnet, doch spricht der Artikel nicht ausdrücklich von der PPC als der für den Erlass spezifischer Vorschriften zuständige Stelle.[18] Aus Zeitmangel war der EDSA nicht in der Lage, die zu diesem Punkt vorhandenen Nachweise zusammenzutragen, zu überprüfen und zu analysieren.

49. **Angesichts der Bedeutung dieses Themas nimmt der EDSA die wiederholten Zusagen und Zusicherungen der Europäischen Kommission und der japanischen Behörden in Bezug auf den verbindlichen und durchsetzbaren Charakter der Ergänzenden Vorschriften zur Kenntnis. Der EDSA fordert die Europäische Kommission auf, ihre Verbindlichkeit und wirksame Anwendung in Japan fortlaufend zu überwachen, da ihr rechtlicher Wert ein wesentliches Element der Angemessenheit EU - Japan ist.**

50. Darüber hinaus verweist die Europäische Kommission in mehreren Abschnitten ihres Entwurfs des Angemessenheitsbeschlusses auf die Leitlinien der PPC („Leitlinien").

51. Obwohl die Europäische Kommission in Erwägungsgrund 16 des Entwurfs des Angemessenheitsbeschlusses klarstellt, dass die Leitlinien eine authorisierte Auslegung des APPI enthalten, verweist sie im selben Erwägungsgrund auf den verbindlichen Charakter dieser Leitlinien: „Nach Auskunft der PPC gelten diese Leitlinien als verbindliche Vorschriften, die integraler Bestandteil des Rechtsrahmens sind und zusammen mit dem Wortlaut des APPI, der Kabinettsverordnung, der Geschäftsordnung der PPC und einer Reihe von F & A der PPC gelesen werden müssen."[19]

52. Soweit der EDSA jedoch weiß, der sich auf dieselben Informationen stützt, sind die von der PPC bereitgestellten Leitlinien nicht rechtsverbindlich. Vielmehr handelt es sich bei ihnen um eine „verbindliche Auslegung" des Gesetzes. Die PPC argumentiert, dass die Leitlinien von den PIHBO in der Praxis befolgt, von der PPC zur Durchsetzung des Gesetzes gegen PIHBO genutzt und von den Gerichten bei der Urteilsfindung herangezogen werden. Diese Elemente sind jedoch kein hinreichender Beweis dafür, dass es sich bei den Leitlinien um rechtsverbindliche Normen handelt.

[18] In einem im Juli 2018 veröffentlichten Artikel, als die Ergänzenden Vorschriften noch in der Entwurfsphase waren, hieß es, die Rechtsverbindlichkeit dieser Vorschriften würde wohl Gegenstand einer internen Debatte im Land werden. Vgl. Fujiwara S., Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (July 2018): p. 19.

[19] Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan, in der dem EDSA am 13. November 2018 übermittelten Fassung, Erwägungsgrund 16.

53. **Der EDSA würde Klarstellungen in dem Angemessenheitsbeschluss in Bezug auf den verbindlichen Charakter der Leitlinien der PPC begrüßen, und er ersucht die Europäische Kommission, diesen Aspekt aufmerksam zu überwachen.**

54. Nach Angaben der PPC werden die Leitlinien in der Praxis dennoch angewandt, da es sich hierbei um örtliche Gepflogenheiten handelt. Die PPC führt an, dass die japanischen Gerichte die Leitlinien der PPC bei der Abfassung ihrer Urteile im Zusammenhang mit der Anwendung der APPI-Vorschriften heranziehen. Die Europäische Kommission verweist auf ein Gerichtsurteil[20] aus dem Jahr 2006 als Beweis dafür, dass sich die japanischen Gerichte für ihre Feststellungen auf Leitlinien stützen. Trotz der Tatsache, dass dem EDSA dieses Gerichtsurteil nicht vorgelegt wurde, würde es der EDSA begrüßen, wenn die Europäische Kommission – sofern verfügbar – ein Gerichtsurteil jüngeren Datums entweder im Bereich Datenschutz oder in einem anderen Bereich vorlegen könnte, in dem die japanischen Gerichte die Leitlinien der PPC oder andere ähnliche Leitlinien als Grundlage für ihre Entscheidung herangezogen haben.

2.3.5 Regelmäßige Überprüfung der Angemessenheitsfeststellung

55. Gemäß Artikel 45 Absatz 3 DSGVO muss eine regelmäßige Überprüfung mindestens alle vier Jahre erfolgen. Gemäß des Referenzpapiers zur Angemessenheit des EDSA[21] handelt es sich dabei um einen allgemeinen Zeitrahmen, der je nach Drittland oder internationaler Organisation, für die ein Angemessenheitsbeschluss vorliegt, anzupassen ist. Je nach den besonderen Umständen des Einzelfalls kann ein kürzerer Überprüfungszyklus gerechtfertigt sein. Zudem können einzelne Vorfälle oder andere Informationen über den Rechtsrahmen des betreffenden Drittlands bzw. der betreffenden internationalen Organisation oder diesbezügliche Änderungen eine vorzeitige Überprüfung erforderlich machen. Außerdem scheint es angebracht, bei gänzlich neuen Angemessenheitsbeschlüssen recht zeitnah eine erste Überprüfung durchzuführen und den Überprüfungszyklus dann ergebnisabhängig nach und nach anzupassen.

56. Unter Berücksichtigung einer Reihe von Faktoren, einschließlich der Tatsache, dass das APPI 2017 in Kraft getreten ist, dass die PPC 2016 eingesetzt wurde und dass noch immer keine Informationen oder Belege zur praktischen Anwendung der Ergänzenden Vorschriften vorliegen, **fordert der EDSA die Europäische Kommission auf, diese Angemessenheitsfeststellung (mindestens) alle zwei Jahre zu überprüfen (und nicht alle vier Jahre, wie im vorliegenden Entwurf des Angemessenheitsbeschlusses vorgeschlagen).**

2.3.6 Von Japan eingegangene internationale Verpflichtungen

57. Gemäß Artikel 45 Absatz 2 Buchstabe c DSGVO und des Referenzpapiers zur Angemessenheit[22] berücksichtigt die Europäische Kommission bei der Bewertung der Angemessenheit des Schutzniveaus eines Drittlands unter anderem die von dem betreffenden Drittland eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten sowie die Umsetzung derartiger Verpflichtungen. Außerdem sollte der Beitritt des Drittlands zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der

[20] Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan, in der dem EDSA am 13. November 2018 übermittelten Fassung, S. 5, Fußnote 16, Osaka District Court, decision of 19 May 2006, Hanrei Jiho, Vol. 1948, p. 122.
[21] WP254, S. 4.
[22] WP254, S. 3.

automatischen Verarbeitung personenbezogener Daten („Konvention Nr. 108+“[23]) und dessen Zusatzprotokoll berücksichtigt werden.

58. **Diesbezüglich stellt der EDSA fest, dass Japan Beobachter im Beratenden Ausschuss der Konvention Nr. 108+ ist.**

2.3.7 Befugnisse der Datenschutzbehörden[24], vor Gericht gegen die Gültigkeit eines Angemessenheitsbeschlusses zu klagen

59. Der EDSA betont, dass zwar im Erwägungsgrund 179 des Entwurfs des Angemessenheitsbeschlusses nur Fälle erwähnt werden, in denen eine Datenschutzbehörde eine Beschwerde erhalten hat, mit der die Vereinbarkeit eines Angemessenheitsbeschlusses mit den Grundrechten des Einzelnen auf Privatsphäre und Datenschutz in Frage gestellt wird, doch ist diese Aussage als Beispiel für Situationen zu verstehen, in denen eine Datenschutzbehörde die Angelegenheit vor ein nationales Gericht bringen kann, was auch ohne Beschwerde möglich sein könnte, und nicht als Einschränkung der Befugnisse, die den Datenschutzbehörden gemäß der DSGVO und den nationalen Rechtsvorschriften der Mitgliedstaaten in dieser Hinsicht zustehen. Die Bestimmungen der DSGVO betreffen sowohl die Befugnis zur Aussetzung von Datenübermittlungen, auch dann, wenn sie auf einem Angemessenheitsbeschluss beruhen, als auch zur Einreichung einer Klage bezüglich der Gültigkeit eines Angemessenheitsbeschlusses; dies ist nicht auf Fälle beschränkt, in denen sie eine Beschwerde erhalten haben, wenn ihr nationales Recht ihnen die Befugnis verleiht, im Einklang mit den einschlägigen Bestimmungen der DSGVO dies umfassender und unabhängig von einer Beschwerde zu tun.

60. **Der EDSA fordert die Europäische Kommission auf, in ihrem Entwurf des Angemessenheitsbeschlusses klarzustellen, dass die Befugnis der Aufsichtsbehörden, nach einer Beschwerde gegen die Gültigkeit eines Angemessenheitsbeschlusses zu klagen, lediglich ein Beispiel für die umfassenderen Befugnisse der Datenschutzbehörden ist, die sich aus der DSGVO ergeben, zu denen auch die Befugnis gehört, Datenübertragungen auszusetzen und eine Klage gegen die Gültigkeit eines Angemessenheitsbeschlusses auch ohne eine Beschwerde zu erheben, sollte ihr nationales Recht dies vorsehen.**

3 KOMMERZIELLE ASPEKTE

3.1 Inhaltliche Grundsätze

61. Kapitel 3 des Referenzpapiers zur Angemessenheit befasst sich mit den „inhaltlichen Grundsätzen“. Das System eines Drittlandes oder einer internationalen Organisation muss diese enthalten, damit das gebotene Schutzniveau als im Wesentlichen gleichwertig mit dem durch das EU-Recht garantierten Niveau gelten kann. Der EDSA erkennt an, dass das japanische Rechtssystem bei der Wahrung des Rechts auf Privatsphäre einen anderen Ansatz verfolgt als die DSGVO. Obwohl das Recht auf Privatsphäre nicht *per se* in der japanischen Verfassung verankert ist, wurde es im Wege der Rechtsprechung als Verfassungsrecht anerkannt, wie auch in dem Beschluss der Europäischen Kommission ausgeführt.[25]

[23] Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, Übereinkommen Nr. 108+, 18. Mai 2018.
[24] Rechtssache C-362/14, Maximillian Schrems / Data Protection Commissioner, 6. Oktober 2015.
[25] Dem EDSA lag keine englische Übersetzung dieser Gerichtsentscheidung vor. Siehe Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates

62. Insbesondere aufgrund der Tatsache, dass sich der japanische Ansatz merklich vom europäischen unterscheidet, muss sorgfältig beobachtet werden, ob nicht nur einzelne Aspekte, sondern auch das gesamte System ein „im Wesentlichen gleichwertiges“ Schutzniveau bietet. Dies bedeutet, dass potenzielle „Defizite“ bei einem inhaltlichen Grundsatz durch einige andere Aspekte ausgeglichen werden könnten, die angemessene Kontrollmechanismen bieten.

3.1.1 Begriffe

63. Auf der Grundlage des Referenzpapiers zur Angemessenheit sollten in dem System eines Drittlands grundlegende Datenschutzkonzepte und/oder -grundsätze gegeben sein. Die in der DSGVO verwendete Terminologie muss dabei zwar nicht übernommen werden, doch sollten sie die Begriffe, die im europäischen Datenschutzrecht verankert sind, widerspiegeln und mit diesen im Einklang stehen. Die Datenschutz-Grundverordnung enthält beispielsweise folgende wichtige Begriffe: „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „Empfänger“ und „sensible Daten“.[26]

64. Das APPI enthält ebenfalls eine Reihe von Definitionen, unter anderem für die Begriffe „personenbezogene Informationen“, „personenbezogene Daten“, „Betreiber von Unternehmen für die Verarbeitung personenbezogener Daten“. **Anscheinend enthält das APPI jedoch keine Definition des Begriffs „Umgang mit personenbezogenen Daten“, der dem Begriff „Verarbeitung personenbezogener Daten“ ähnelt.**

65. Zur Definition des Begriffs „Umgang mit personenbezogenen Daten“ übermittelte die PPC eine schriftliche Antwort auf die Anfrage des EDSA zu dieser Definition. Die Europäische Kommission zitierte diese Antwort im Entwurf des Beschlusses der Kommission: „*Das APPI verwendet zwar nicht den Begriff „Verarbeitung“, stützt sich aber auf den gleichwertigen Begriff des „Umgangs “, der nach den von der PPC erhaltenen Informationen „jede Tätigkeitim Zusammenhang mit personenbezogenen Daten“ umfasst, einschließlich des Erwerbs, der Eingabe, der Erhebung, der Organisation, der Lagerung, der Bearbeitung/Verarbeitung, der Erneuerung, der Ausgabe, der Sicherung, der Verwendung oder der Bereitstellung personenbezogener Informationen.*“[27]

66. Da jedoch die Fundstelle mit dem Wortlaut dieser Definition nicht angegeben wurde, fordert der EDSA **die Europäische Kommission auf, genau zu überwachen, dass die Definition des oben genannten Begriffs, wie sie von der PPC angegeben wird, in der Praxis tatsächlich befolgt wird.**

3.1.1.1 Begriff des Auftragsverarbeiters und Pflichten eines „Treuhänders“

67. Wie bereits erwähnt, verlangt das Referenzpapier zur Angemessenheit, dass im Rechtsrahmen eines Drittlands grundlegende Datenschutzkonzepte und/oder -grundsätze gegeben sein sollten.

68. Das APPI enthält eine Definition des Begriffs „Betreiber von Unternehmen für die Verarbeitung personenbezogener Daten“, der der Europäischen Kommission zufolge sowohl den Begriff „für die Verarbeitung Verantwortlicher“ als auch den Begriff „Auftragsverarbeiter“ im Sinne der DSGVO umfasst und zwischen den beiden keinen Unterschied macht.[28] Allerdings enthält das APPI in seinem

---

über die Angemessenheit des Datenschutzniveaus in Japan, in der dem EDSA am 13. November 2018 übermittelten Fassung, Fußnote 9.

[26] WP254, S. 5.

[27] Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan, in der dem EDSA am 13. November 2018 übermittelten Fassung, Erwägungsgrund 17.

[28] Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan, in der dem EDSA am 13. November 2018 übermittelten Fassung, Erwägungsgrund 35.

Artikel 22 auch den Begriff „Treuhänder“, der in gewisser Weise dem Begriff des Auftragsverarbeiters nach der DSGVO entspricht.

69. Wie die PPC in ihren Antworten an den EDSA erläutert, und wie es auch in dem Entwurf des Angemessenheitsbeschlusses der Europäischen Kommission heißt, gilt ein Treuhänder als gleichwertig mit einem Auftragsverarbeiter im Sinne der DSGVO – eine Person, die von einem PIHBO mit dem Umgang mit personenbezogenen Daten betraut wird. Dieser Treuhänder hat dieselben Pflichten und Rechte wie jeder PIHBO, einschließlich der in den Ergänzenden Vorschriften für aus der EU übermittelte personenbezogene Daten niedergelegten. Der PIHBO, der einen Treuhänder mit dem Umgang mit personenbezogenen Daten betraut, ist verpflichtet, „die erforderliche und angemessene Aufsicht“[29] über den Treuhänder auszuüben.

70. **Der EDSA fordert die Europäische Kommission auf, den Status und die Pflichten des Treuhänders zu erläutern, wenn der Treuhänder die Zwecke und Mittel der Verarbeitung ändert, und klarzustellen, ob die Einwilligung der betroffenen Person nach wie vor eine notwendige Voraussetzung für eine solche Änderung des Zwecks oder der Mittel ist.[30]**

3.1.1.2 Begriff der gespeicherten personenbezogenen Daten

71. Das APPI enthält den Begriff „gespeicherte personenbezogene Daten“, die als Unterkategorie personenbezogener Daten gelten. Gemäß dem APPI gelten die Bestimmungen über die Rechte der betroffenen Person[31] nur für gespeicherte personenbezogene Daten. Eine Definition des Begriffs von „gespeicherte personenbezogene Daten“ findet sich in Artikel 2 Absatz 7 des APPI.

72. Gespeicherte personenbezogene Daten sind alle anderen Daten außer personenbezogenen Daten, die i) innerhalb eines Zeitraums von höchstens sechs Monaten zu löschen sind[32] oder ii) unter die Ausnahmen in Artikel 4 der Kabinettsverordnung fallen und der Öffentlichkeit oder anderen Interessen schaden könnten, wenn ihr Vorhandensein oder ihr Fehlen bekannt werden.

73. Die Ergänzende Vorschrift 2 sieht vor, dass *„personenbezogene Daten, die aus der EU auf der Grundlage eines Angemessenheitsbeschlusses übermittelt werden, ohne Rücksicht auf den Zeitraum, innerhalb dessen sie zu löschen sind, als gespeicherte personenbezogene Daten zu behandeln sind“.*

74. Allerdings müssen personenbezogene Daten, die unter die Ausnahmen von Artikel 4 der Kabinettsverordnung fallen, nicht als gespeicherte personenbezogene Daten behandelt werden und gelten die Rechte der betroffenen Personen nicht.

75. Gemäß Artikel 23 DSGVO können, wie auch gemäß Artikel 4 der Kabinettsverordnung, durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterliegt, die für ihn geltenden Verpflichtungen und die der betroffenen Person zur Verfügung stehenden Rechte eingeschränkt werden. Dies kann im Wege von Gesetzgebungsmaßnahmen geschehen. Solche Beschränkungen müssen den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen.

[29] Artikel 22 des geänderten Gesetzes über den Schutz personenbezogener Informationen (APPI), das am 30. Mai 2017 in Kraft gesetzt wurde.
[30] Artikel 23 Absatz 5 Buchstabe i APPI. Siehe auch weiter unten den Abschnitt zum Grundsatz der Transparenz.
[31] Artikel 27-30 APPI.
[32] Änderung der Kabinettsverordnung zur Inkraftsetzung des Gesetzes über den Schutz personenbezogener Daten (Kabinettsverordnung), in Kraft gesetzt am 30. Mai 2017, Artikel 5.

76. Zu dem Inhalt der Ausnahmen nach Artikel 4 der Kabinettsverordnung wurden dem EDSA keine ausreichenden Unterlagen über diese Beschränkungen oder zusätzlichen Elemente zur Klärung des Geltungsbereichs dieser Bestimmungen zur Verfügung gestellt.[33] Der EDSA ist nicht in der Lage zu beurteilen, ob diese Beschränkungen der Rechte der betroffenen Personen auf das begrenzt sind, was nach EU-Recht als unbedingt notwendig und verhältnismäßig gilt, und somit im Wesentlichen den Rechten gleichwertig sind, die betroffenen Personen in der EU zustehen.

77. **Da einige relevante Unterlagen nicht vorliegen, würde der EDSA ferner Zusicherungen der Europäischen Kommission zu der Frage begrüßen, ob die Beschränkungen der Rechte des Einzelnen (insbesondere des Rechts auf Auskunft, Berichtigung und Widerspruch) in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind und den Wesensgehalt der Grundrechte achten.**

78. Eine grundlegende Anforderung der DSGVO besagt, dass personenbezogene Daten während ihres gesamten „Lebenszyklus" geschützt werden müssen.

79. Unter Berücksichtigung der Tatsache, dass die Ergänzenden Vorschriften nur für aus der EU übermittelte personenbezogene Daten gelten, würde der EDSA weitere Informationen über die praktische Umsetzung dieser Vorschriften durch die PIHBO begrüßen, insbesondere zu Fällen, in denen diese Daten nach ihrer ersten Übermittlung nach Japan an einen anderen PIHBO weiterübermittelt werden.

80. Die Europäische Kommission hat in Erwägungsgrund 15 ihres Entwurfs des Angemessenheitsbeschlusses klargestellt, dass PIHBO, die personenbezogene Daten aus der EU erhalten und/oder weiterverarbeiten, nach dem Gesetz verpflichtet sein werden, die Ergänzenden Vorschriften einzuhalten, und dass sie hierzu sicherstellen müssen, dass sie solche personenbezogenen Daten während ihres gesamten „Lebenszyklus" identifizieren können.

81. Die PPC[34] hat in ihren Antworten erklärt, dass eine solche Identifizierung mittels technischer (Kennzeichnung) oder organisatorischer Methoden (Speicherung der Daten aus der EU in einer eigenen Datenbank) erfolgen wird.

82. In Fußnote 14 ihres Entwurfs des Angemessenheitsbeschlusses erläutert die Europäische Kommission, dass PIHBO Angaben zum Ursprung der EU-Daten so lange speichern müssen, wie dies für die Einhaltung der Ergänzenden Vorschriften erforderlich ist. Dies ist auch in Artikel 26 Absätze 1, 3 und 4 des APPI verankert, wo es heißt, dass ein PIHBO verpflichtet ist, die Quelle dieser Daten und alle Begleitumstände des Erwerbs dieser Daten zu bestätigen und aufzuzeichnen.

83. Der EDSA stellt jedoch fest, dass gemäß Artikel 18 der Vorschriften der PPC[35] die Aufzeichnungspflichten von PIHBO auf höchstens drei Jahre für Fälle begrenzt sind, die nicht unter die spezifischen Aufzeichnungsmethoden gemäß Artikel 16 der PPC-Vorschriften fallen (Verwendung eines schriftlichen Dokuments, elektromagnetische Aufzeichnung oder Mikrofilm). Dies stellt auch die Europäische Kommission in Erwägungsgrund 71 ihres Entwurfs des Angemessenheitsbeschlusses fest: *„Wie in Artikel 18 der PPC-Vorschriften festgelegt, müssen diese Aufzeichnungen je nach den Umständen für einen Zeitraum von einem bis drei Jahren aufbewahrt werden."*

[33] Dem EDSA liegen die in Erwägungsgrund 53 des Entwurfs des Angemessenheitsbeschlusses aufgeführten Entscheidungen des Obersten Gerichtshofs nicht vor.
[34] Anhang III dieser Stellungnahme.
[35] Durchführungsvorschriften für das Gesetz über den Schutz personenbezogener Daten (PPC-Vorschriften), in Kraft gesetzt am 30. Mai 2017, Artikel 16.

84. Auch wenn, wie die Europäische Kommission in Fußnote 14 ihres Entwurfs eines Angemessenheitsbeschlusses feststellt, es den PIHBO nicht untersagt ist, Aufzeichnungen über den Ursprung der Daten länger als drei Jahre aufzubewahren, um ihren Verpflichtungen nach der Ergänzenden Vorschrift 2 nachkommen zu können, wird dies doch weder in den japanischen Rechtsvorschriften noch in den Ergänzenden Vorschriften deutlich. Nach Auffassung des EDSA besteht die Gefahr, dass die PIHBO tatsächlich Artikel 18 der PPC-Vorschriften einhalten, auch wenn sie aus der EU stammende Daten verarbeiten. Dies liegt in erster Linie daran, dass es derzeit aus der Sichtweise des EDSA und nach Durchsicht der verfügbaren Unterlagen keine Bestimmung gibt, die die PIHBO dazu verpflichtet, stattdessen die Ergänzenden Vorschriften einzuhalten. Dies würde dazu führen, dass die aus der EU übermittelten Daten nicht mehr durch die in den Ergänzenden Vorschriften enthaltenen zusätzlichen Schutzvorkehrungen geschützt werden.

85. **Der EDSA fordert die Europäische Kommission auf, den wirksamen Schutz personenbezogener Daten, die auf der Grundlage des Entwurfs des Angemessenheitsbeschlusses aus der EU nach Japan übermittelt werden, während ihres gesamten „Lebenszyklus" genau zu überwachen, auch wenn die japanischen Rechtsvorschriften eine Aufzeichnungspflicht hinsichtlich des Ursprungs der Daten für einen Zeitraum von höchstens drei Jahren vorsehen.**

3.1.2 Voraussetzungen für eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu legitimen Zwecken

86. Gemäß des Referenzpapiers zur Angemessenheit und in Anlehnung an die DSGVO muss die Verarbeitung auf rechtmäßige und faire Weise für legitime Zwecke erfolgen.[36] Die rechtlichen Voraussetzungen, unter denen personenbezogene Daten rechtmäßig, nach Treu und Glauben und auf legitime Weise verarbeitet werden dürfen, sollten hinreichend klar dargelegt werden. Im europäischen Rahmen werden mehrere solche rechtlichen Voraussetzungen anerkannt, darunter Bestimmungen des nationalen Rechts, die Einwilligung der betroffenen Person, die Erfüllung eines Vertrags oder das berechtigte Interesse des für die Verarbeitung Verantwortlichen oder eines Dritten, das keinen Vorrang vor den Interessen des Einzelnen hat.

87. Gemäß dem APPI spielt die Zustimmung eine zentrale Rolle im japanischen Datenschutzrecht. Die Einwilligung ist die zentrale rechtliche Voraussetzung für die Verarbeitung personenbezogener Daten in Japan und auch eine der wichtigsten rechtlichen Voraussetzungen für Übermittlungen personenbezogener Daten aus Japan in ein Drittland. Darüber hinaus ist die Einwilligung bei einer Änderung des Verarbeitungszwecks erforderlich.

88. Gemäß der Ergänzenden Vorschrift 3 wird die Rechtsgrundlage für die Verarbeitung von aus der EU nach Japan übermittelten personenbezogenen Daten die Rechtsgrundlage sein, auf der die Daten an Japan übermittelt werden. Wenn der PIHBO diese Daten zu einem anderen Zweck verarbeiten möchte, muss er vorab die Einwilligung der betroffenen Person einholen.

89. Nach Auffassung des EDSA muss die Qualität der Einwilligung, insbesondere aufgrund ihrer zentralen Rolle im japanischen Rechtsrahmen, die grundlegenden Anforderungen an den Begriff „Einwilligung" erfüllen, d. h., sie muss gemäß dem EU-Recht eine *„freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung (...)"* sein. Die betroffene Person kann diese Einwilligung widerrufen; dies ist eine wesentliche Garantie dafür, dass der freie Wille der betroffenen Person jederzeit gewahrt ist.[37] Das Widerrufsrecht als obligatorisches Element der

[36] WP254, S. 5.

[37] Artikel 4 Absatz 11 DSGVO. Weitere Informationen sind den einschlägigen Leitlinien des EDSA zum Thema Einwilligung zu entnehmen, WP259 vom 10. April 2018.

Einwilligung scheint im japanischen Rechtsrahmen zu fehlen. Nach den Leitlinien der PPC[38] ist der Widerruf nur „wünschenswert“ und von „Merkmalen, Größe und Status der Geschäftstätigkeit“ abhängig.

3.1.3 Grundsatz der Transparenz

90. Gemäß Artikel 5 DSGVO ist Transparenz ein tragender Grundsatz des EU-Datenschutzsystems.[39] In dem Referenzpapier zur Angemessenheit wird „Transparenz“ ausdrücklich als einer der Grundsätze genannt, die bei der Bewertung des von einem Drittland gebotenen im Wesentlichen gleichwertigen Schutzniveaus zu berücksichtigen sind. Mit dem Grundsatz der Transparenz und Fairness soll sichergestellt werden, dass die betroffene Person die Kontrolle über ihre Daten hat, und zu diesem Zweck werden der betroffenen Person in der Regel proaktiv Informationen zur Verfügung gestellt. Im Fall des Datenschutzschilds hat die Artikel 29-Datenschutzgruppe[40] in ihrer Stellungnahme 1/2016 auf Anhang II, Punkt II 1 b des Datenschutzschild-Abkommens (Information des Betroffenen) Bezug genommen und erklärt, dass in dem Fall, in dem die Daten nicht direkt erhoben werden, eine Organisation die betroffene Person „an der Stelle, an der die Daten von der Organisation erfasst werden“ informieren sollte (Abschnitt 2.2.1.a). Ein weiteres Kriterium ist die Zugänglichkeit der Datenschutzerklärung für die Öffentlichkeit (siehe Abschnitt 2.2.1.b). Allerdings galt es bereits nach der Richtlinie 95/46/EG als erforderlich, die betroffene Person direkt zu unterrichten.

91. Ein erstes Problem ist die Form, in der betroffene Personen nach dem APPI informiert werden. Gemäß Artikel 27 Absatz 1 APPI ist ein PIHBO verpflichtet, die in Artikel 27 Absatz 1 APPI beschriebenen Angaben zu machen, indem er „sie in einen Zustand bringt, in der ein Betroffener sie erfahren kann“. Aus dieser Formulierung geht jedoch nicht eindeutig hervor, in welchem Umfang der PIHBO positive Maßnahmen ergreifen muss, um die betroffene Person tatsächlich zu informieren.

92. **Der EDSA fordert die Kommission auf, die Bedeutung der Formulierung „erfahren kann“ zu präzisieren und zu klären, ob das APPI generell die Pflicht vorsieht, betroffene Personen tatsächlich zu informieren.**

93. Darüber hinaus gibt es nach dem Referenzpapier zur Angemessenheit möglicherweise Einschränkungen bei den Informationen, die der betroffenen Person zur Verfügung zu stellen sind, ähnlich wie in Artikel 23 DSGVO. Ferner sieht Artikel 14 Absatz 5 DSGVO eine Ausnahme von dem Recht auf Informationen vor, wenn die Erteilung dieser Informationen voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. Doch selbst in einem solchen Fall muss der für die Verarbeitung Verantwortliche bestimmte Informationen bereitstellen, beispielsweise indem er „verallgemeinerte“ Informationen öffentlich zugänglich macht.

---

[38] Konsortium für rechtliche und technische Forschung und Analyse (Data Protection Legal and Technical Research and Analysis Consortium), An assessment of the level of protection of personal data provided under Japanese law (Bewertung des nach japanischem Recht gewährleisteten Schutzniveaus für personenbezogene Daten), S. 46: „Aus der Sicht des Schutzes der Rechte und der Interessen von Betroffenen wie der Verbraucher ist es ferner wünschenswert, dass bei Eingang einer Anfrage eines Betroffenen betreffend die gespeicherten personenbezogenen Daten auf die Forderung des Betroffenen so eingegangen wird, dass der Versand von Direktwerbung gestoppt usw. oder freiwillig die Nutzung eingestellt wird usw., und zwar unter Berücksichtigung der Merkmale, der Größe und des Status der Geschäftstätigkeiten.“

[39] WP254, Kapitel 3, Punkt 7, S. 6; siehe ferner Erwägungsgrund 39 der DSGVO.

[40] Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie war ein unabhängiges europäisches Beratungsgremium für Datenschutz und Schutz der Privatsphäre. Ihre Aufgaben sind beschrieben in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG. Aus der Artikel 29-Datenschutzgruppe (WP29) ist nunmehr der EDSA geworden.

Darüber hinaus ist die betroffene Person zu benachrichtigen, wenn das Risiko nicht mehr besteht.[41] Diese Aspekte sind wichtig, um das Grundprinzip der Fairness zu wahren.

94. Gemäß Artikel 23 des APPI hat ein PIHBO die betroffene Person generell vorab über die Übermittlung ihrer Daten an einen Dritten zu informieren, und zwar entweder implizit bei der Einholung ihrer Einwilligung oder ausdrücklich durch eine Opt-out-Erklärung. Der EDSA geht davon aus, dass es keine Mitteilung an die betroffene Person gibt, mit der sie davon in Kenntnis gesetzt wird, dass ihre Daten nicht nach dem APPI gespeichert werden, weil sie unter die Ausnahmen in Artikel 4 der Kabinettsverordnung fallen. Das hat zur Folge, dass sie ihre Rechte nicht in vollem Umfang wahrnehmen kann. In den Fällen von Artikel 18 Absatz 4 APPI werden die betroffenen Personen ebenfalls nicht informiert.

95. **Der EDSA erkennt an, dass die Rechte für legitime Ziele von PIHBO und staatlichen Behörden beschränkt werden können. Gleichzeitig ist der EDSA der Ansicht, dass zumindest allgemeine Informationen über die Möglichkeit einer Beschränkung der Rechte für die im Gesetz genannten Ziele vorliegen sollten und dass die betroffene Person benachrichtigt werden sollte, wenn die Risiken, aufgrund derer die Informationen eingeschränkt werden, nicht mehr bestehen.**

96. Auf weitere Aspekte der Transparenz wird weiter unten eingegangen. Dabei handelt es sich um Risiken, die mit einer Übermittlung in ein Drittland verbunden sind[42], und um Informationen über die Logik der Verarbeitung im Zusammenhang mit der automatisierten Entscheidungsfindung einschließlich Profiling.[43]

3.1.4 Beschränkungen bei Weiterübermittlungen

97. Der EDSA begrüßt die Bemühungen der japanischen Behörden und der Europäischen Kommission um eine Verbesserung des Schutzniveaus bei Weiterübermittlungen in der Ergänzenden Vorschrift 4, der zufolge eine Weiterübermittlung von aus der EU übermittelten Daten an ein Drittland auf der Grundlage von APEC-CBPR ausgeschlossen ist. Darüber hinaus räumt der EDSA ein, dass sich die Europäische Kommission in den Erwägungsgründen 177 und 184 ihres neuen Entwurfs eines Angemessenheitsbeschlusses dazu verpflichtet hat, den Angemessenheitsbeschluss auszusetzen, wenn bei Weiterübermittlungen keine Kontinuität des Schutzes gewährleistet sein würde. Dessen ungeachtet möchte der EDSA zwei Punkte zu diesen Übermittlungen personenbezogener Daten aus der EU aus Japan an Drittländer ansprechen.

98. **Die im japanischen Recht vorgesehene Nutzung der Einwilligung als Grundlage für die Übermittlung von Daten aus Japan in ein Drittland wirft Bedenken auf, da nach Ansicht des EDSA die Informationen, die der betroffenen Person in der EU vor der Einwilligung erteilt wurden, nicht umfassend sein dürften.**

99. Nach Artikel 24 APPI darf die Übermittlung personenbezogener Daten an einen Dritten außerhalb Japans nur mit vorheriger Einwilligung der betreffenden Person erfolgen. In der Ergänzenden Vorschrift 4 ist festgelegt, dass betroffene Personen in der EU Informationen über die Umstände der Übermittlung erhalten müssen, die sie benötigen, um über ihre Einwilligung entscheiden zu können.

100. Die Europäische Kommission kommt in ihrem Entwurf des Angemessenheitsbeschlusses zu dem Schluss, dass die Ergänzende Bestimmung 4 eine nach besonders gründlicher Information der

[41] Tele2, Verbundene Rechtssachen C-203/15 und C-698/15, Urteil des Gerichtshofs vom 21. Dezember 2016, Rn. 121, und Digital Rights Ireland, Verbundene Rechtssachen C-293/12 und C-594/12, Urteil des Gerichtshofs vom 8. April 2014, Rn. 54-62.
[42] Siehe Abschnitt 2.1.4.
[43] Siehe Abschnitt 2.1.6.

betroffenen Person in der EU erteilte Einwilligung gewährleistet[44], da sie über die Tatsache aufgeklärt wird, dass die Daten ins Ausland und in welches Bestimmungsland genau sie übermittelt werden. Dies würde es der betroffenen Person ermöglichen, das mit der Übermittlung verbundene Risiko für den Schutz der Privatsphäre zu bewerten.

101. Nach dem Grundsatz der Transparenz des Referenzpapiers zur Angemessenheit ist bei der Information des Einzelnen ein bestimmtes Maß an Fairness zu gewährleisten. Im Zusammenhang mit Weiterübermittlungen auf der Grundlage einer Einwilligung ist der EDSA der Auffassung, dass im Sinne eines solchen angemessenen Maßes an Fairness betroffene Personen ausdrücklich über die möglichen Risiken solcher Übermittlungen aufgeklärt werden sollten, die sich aus dem Fehlen eines angemessenen Schutzes in dem Drittland und dem Fehlen geeigneter Garantien vor der Einwilligung ergeben. Dieser Hinweis sollte beispielsweise darüber informieren, dass es in dem Drittland möglicherweise keine Aufsichtsbehörde und/oder Grundsätze des Datenschutzes gibt und/oder dass die Rechte der betroffenen Person in dem Drittland nicht gewahrt sind.[45] Für den EDSA ist die Bereitstellung dieser Informationen von wesentlicher Bedeutung, damit die betroffenen Personen in der Lage sind, in umfassender Kenntnis dieser spezifischen Fakten ihre Einwilligung zu der Übermittlung zu geben.[46]

102. Die Einwilligung nach Aufklärung ist auch im Zusammenhang mit den sektorspezifischen Ausschlüssen von Bedeutung. Der Angemessenheitsbeschluss erstreckt sich nicht auf bestimmte Arten der Verarbeitung durch bestimmte Einrichtungen wie Universitäten für die Verarbeitung personenbezogener Daten für akademische Zwecke. Die Bedenken des EDSA betreffen hier das spezifische Szenario, dass Daten, die aus der EU nach dem Angemessenheitsbeschluss übermittelt werden – beispielsweise die Personaldaten von Erasmus-Studierenden in Japan – dann für einen anderen Zweck verwendet werden, der nicht in den Geltungsbereich des Angemessenheitsbeschlusses fällt (z. B. zu Forschungszwecken), und zwar mit der Einwilligung der betroffenen Person – und daher nicht mehr unter den zusätzlichen Schutz durch die Ergänzenden Vorschriften fallen.

103. Die Europäische Kommission stellt in Erwägungsgrund 38 ihres Entwurfs des Angemessenheitsbeschlusses fest, dass ein solches Szenario gegebenenfalls in den Bereich der Weiterübermittlung fällt und dass der PIHBO der betroffenen Person alle erforderlichen Informationen zur Verfügung stellen muss, bevor sie ihre Einwilligung erteilt, einschließlich der Tatsache, dass die personenbezogenen Daten nicht unter den Schutz der APPI-Vorschriften fallen würden.

104. In der Ergänzenden Vorschrift 4 wird vom PIHBO nur verlangt, die Einwilligung der betroffenen Person einzuholen, nachdem diese über die Umstände der Übermittlung die Informationen erhalten hat, die sie benötigt, um über ihre Einwilligung entscheiden zu können.

105. **Der EDSA fordert die Europäische Kommission auf, dafür zu sorgen, dass die Informationen, die der betroffenen Person „zu den Umständen der Übermittlung" zur Verfügung gestellt werden, auch Informationen über mögliche Risiken von Übermittlungen enthalten, die sich aus dem Fehlen eines angemessenen Schutzes in dem betreffenden Drittland und aus dem Fehlen angemessener Garantien oder, im Falle sektorspezifischer Ausschlüsse, dem Fehlen von Schutzvorkehrungen in den Ergänzenden Vorschriften und im APPI ergeben.**

[44] Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan, in der dem EDSA am 13. November 2018 übermittelten Fassung, Erwägungsgrund 76.
[45] Leitlinien des EDSA 2/2018 über Ausnahmen von Artikel 49 der Verordnung (EU) 2016/679, 25. Mai 2018, S. 8.
[46] Leitlinien des EDSA 2/2018 über Ausnahmen von Artikel 49 der Verordnung (EU) 2016/679, 25. Mai 2018, S. 8.

106. **Weiterübermittlungen personenbezogener Daten können an Drittländer erfolgen, die möglicherweise später Gegenstand eines japanischen Angemessenheitsbeschlusses werden.**

107. Unbeschadet der in Artikel 23 Absatz 1 APPI festgelegten Ausnahmen können Daten, die ursprünglich aus der EU nach Japan übermittelt wurden, in zwei Fällen ohne Einwilligung von Japan weiter in ein Drittland übermittelt werden:

- Wenn der PIHBO und der Empfänger in einem Drittland in Form eines Vertrags, anderer Formen verbindlicher Vereinbarungen oder verbindlicher Vereinbarungen innerhalb einer Unternehmensgruppe gemeinsam Maßnahmen ergriffen haben, die ein dem APPI in Kombination mit den Ergänzenden Vorschriften gleichwertiges Schutzniveau gewährleisten.[47]
- Wenn das Drittland von der PPC gemäß Artikel 24 APPI und Artikel 11 der PPC-Vorschriften[48] als ein Land anerkannt wurde, das ein dem in Japan garantierten Schutzniveau gleichwertiges Niveau gewährleistet.

108. Der EDSA sieht in Artikel 24 APPI eine eher spezifische Vorschrift mit einer Ausnahme von der allgemeinen Regel in Artikel 23 APPI. Daher teilt der EDSA nicht die Einschätzung der Europäischen Kommission in dem neuen letzten Satz von Erwägungsgrund 78 des Entwurfs des Angemessenheitsbeschlusses, wonach auch in diesen Fällen die Übermittlung an den Dritten weiterhin dem Erfordernis einer Einwilligung nach Artikel 23 Absatz 1 APPI unterliegt.

109. Gemäß Artikel 11 Absatz 1 der PPC-Vorschriften erfordert ein Angemessenheitsbeschluss der PPC materiellrechtliche Standards, die dem APPI gleichwertig sind, deren Umsetzung in dem Drittland gewährleistet ist und die von einer unabhängigen Durchsetzungsbehörde effektiv überwacht werden. Darüber hinaus kann die PPC gemäß Artikel 11 Absatz 2 der PPC-Vorschriften die notwendigen Voraussetzungen für den Schutz der Rechte und Interessen von Personen in Japan vorgeben.

110. In der Ergänzenden Vorschrift 4 heißt es, dass personenbezogene Daten aus der EU ohne weitere Einschränkungen in ein Drittland übermittelt werden können, sofern für dieses Land ein Angemessenheitsbeschluss Japans vorliegt. In Artikel 44 DSGVO ist jedoch festgelegt, dass bei jedweder Übermittlung personenbezogener Daten in ein Drittland die in Kapitel V DSGVO festgelegten Bedingungen einzuhalten sind, also auch bei der etwaigen Weiterübermittlung durch das Drittland an ein anderes Drittland. Das Schutzniveau natürlicher Personen, deren Daten übermittelt werden, darf durch die Weiterübermittlung nicht beeinträchtigt werden.[49] Auch wenn diese Auslegung von der Europäischen Kommission im Entwurf des Angemessenheitsbeschlusses[50] grundsätzlich geteilt wird, scheint ihr nicht vollständig Folge geleistet zu werden. Die Europäische Kommission hat ausgehandelt, dass die Übermittlung von Daten mit Ursprung in der EU an ein Drittland auf der Grundlage der Asiatisch-Pazifischen Wirtschaftskooperation (APEC) – Cross Border Privacy Rules (CBPR) – verboten ist. Angesichts des im Jahr 2014 entwickelten Vergleichsinstruments im Rahmen der EU-Richtlinie zwischen BCR und CBPR, in dem die Anforderungen beider Systeme, ihre Konvergenzen und Unterschiede dargestellt sind (Artikel 29-Datenschutzgruppe, Stellungnahme 02/2014), hat der EDSA

[47] Ergänzende Vorschrift 4 Ziffer ii.

[48] Durchführungsvorschriften für das Gesetz über den Schutz personenbezogener Daten, 30. Mai 2017. Die Europäische Kommission hat dem EDSA eine englische Übersetzung des neuen Artikels 11 übermittelt, doch ist dieser Artikel bisher noch nicht veröffentlicht worden.

[49] WP254, S. 6.

[50] Durchführungsbeschlusses der Kommission vom XXXX gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan, in der dem EDSA am 13. November 2018 übermittelten Fassung, Erwägungsgrund 75.

Bedenken hinsichtlich der Nutzung von CBPR als Instrument für die Weiterübermittlung aus der EU stammender personenbezogener Daten in Länder außerhalb Japans.

111. Allerdings scheinen Weiterübermittlungen aus der EU stammender und an Japan auf der Grundlage eines Angemessenheitsbeschlusses übermittelter personenbezogener Daten von der Europäischen Kommission akzeptiert zu werden, ohne dass der PPC die Möglichkeit eingeräumt würde, erforderlichenfalls die Ergänzenden Vorschriften als Bedingungen für den Schutz der Rechte und Interessen von EU-Bürgern vorzuschreiben. Der EDSA entnimmt Artikel 44 DSGVO, dass der in den Ergänzenden Vorschriften vorgesehene verstärkte Schutz von Daten, die aus der EU nach Japan übertragen werden, immer auf Fälle ausgeweitet werden muss, in denen aus der EU nach Japan übermittelte personenbezogene Daten in ein Drittland weiterübermittelt werden und der Datenschutzrahmen in diesem Land nicht als im Wesentlichen mit der DSGVO gleichwertig anerkannt ist.

112. **Daher fordert der EDSA die Europäische Kommission auf, ihrer Überwachungsfunktion gerecht zu werden und sicherzustellen, dass das Schutzniveau für EU-Daten aufrechterhalten wird, oder eine Aussetzung dieses Angemessenheitsbeschlusses in Betracht zu ziehen, wenn aus der EU nach Japan übermittelte personenbezogene Daten in Drittländer weiterübermittelt werden, für die möglicherweise ein späterer Angemessenheitsbeschluss Japans gilt, wenn diese Drittländer nicht zuvor seitens der EU einer Angemessenheitsprüfung unterzogen wurden bzw. für sie keine Angemessenheitsfeststellung der EU vorliegt.**

3.1.5 Direktwerbung

113. Gemäß der Ergänzenden Vorschrift 3 ist es einem PIHBO untersagt, Daten zum Zwecke der Direktwerbung zu verarbeiten, wenn sie aus der Europäischen Union zu einem anderen Zweck übertragen wurden und die betroffene Person in der EU der Änderung des Verwendungszwecks nicht zugestimmt hat.

114. In dem Referenzpapier zur Angemessenheit heißt es hierzu: „Werden Daten verarbeitet, um Direktwerbung zu betreiben, sollte es für die betroffene Person jederzeit möglich sein, kostenlos Widerspruch gegen die Verarbeitung ihrer Daten zu diesen Zwecken einzulegen." Gemäß Artikel 16 APPI darf ein PIHBO nur dann personenbezogene Daten verarbeiten, wenn die betroffene Person ihre Einwilligung gibt. Der Widerruf der Einwilligung könnte zum gleichen Resultat führen wie das privilegierte Recht auf Widerspruch gegen Direktwerbung.

115. Der japanische Datenschutzrahmen sieht kein privilegiertes Widerspruchsrecht vor, und wie vorstehend in dem Abschnitt über Einwilligung erläutert, ist der Widerruf der Einwilligung nach den PPC-Leitlinien lediglich wünschenswert und bedingt und kann daher nicht als einem Recht auf Widerspruch zu jeder Zeit gleichgestellt werden, wie in dem Referenzpapier zur Angemessenheit verlangt. **Der EDSA fordert die Europäische Kommission auf, Zusicherungen in Bezug auf das Recht auf Widerruf der Einwilligung zu machen und Fälle im Bereich Direktwerbung zu überwachen.**

3.1.6 Automatisierte Entscheidungen und Profiling

116. In dem Referenzpapier zur Angemessenheit heißt es hierzu: „Entscheidungen, die allein auf der Grundlage der automatisierten Verarbeitung (automatisierte Entscheidungen im Einzelfall) einschließlich Profiling beruhen, die eine rechtliche Wirkung für die betroffene Person entfalten oder sie erheblich beeinträchtigen, sind nur unter bestimmten Bedingungen zulässig, die im Rechtsrahmen des Drittlands festzulegen sind." Daher muss jedes Mal, wenn unter den genannten Umständen eine automatisierte Entscheidungsfindung und Profilerstellung durchgeführt werden, eine rechtliche Voraussetzung hierfür bestehen.

117. Im europäischen Rahmen umfassen diese Bedingungen zum Beispiel das Erfordernis, die ausdrückliche Einwilligung[51] der betroffenen Person einzuholen, oder die Notwendigkeit einer solchen Entscheidung zum Abschluss eines Vertrags. Steht die Entscheidung nicht im Einklang mit den im Rechtsrahmen des Drittlands festgelegten Bedingungen, sollte die betroffene Person das Recht haben, ihr nicht zu unterliegen. In jedem Fall sollten nach dem Recht des Drittlands die erforderlichen Garantien gewährleistet werden, einschließlich des Rechts auf Unterrichtung über die besonderen Gründe, die der Entscheidung und der angewandten Logik zugrunde liegen, um unrichtige und unvollständige Angaben zu berichtigen und die Entscheidung anzufechten, falls sie auf der Grundlage einer falschen Sachlage getroffen wurde.

118. Im Beschluss der Kommission wird nur auf den Bankensektor Bezug genommen, für den sektorspezifische Vorschriften[52] für automatisierte Entscheidungen gelten würden. Aus den in Erwägungsgrund 93 des Entwurfs des Angemessenheitsbeschlusses erwähnten umfassenden Leitlinien für die Beaufsichtigung von Großbanken geht hervor, dass die betreffende Person spezifische Erklärungen zu den Gründen für die Ablehnung eines Antrags auf Abschluss eines Darlehensvertrags erhalten muss.

119. Das von der Europäischen Kommission im Entwurf des Angemessenheitsbeschluss (Erwägungsgrund 94) vorgetragene Argument, dass das Fehlen spezifischer Vorschriften über automatisierte Entscheidungen im APPI das Schutzniveau kaum beeinträchtigen dürfte, scheint (beispielsweise) nicht den Fall zu berücksichtigen, in dem aus der EU übermittelte personenbezogene Daten von einem anderen japanischen für die Verarbeitung Verantwortlichen (nicht dem ursprünglichen japanischen Datenimporteur) verarbeitet werden.

120. Es hat daher den Anschein, als gebe es in Japan keine sektorübergreifenden allgemeinen Vorschriften für automatisierte Entscheidungen und Profiling.

121. **Der EDSA fordert die Europäische Kommission auf, Fälle von automatisierten Entscheidungen und Profiling zu überwachen.**

3.2 Verfahrens- und Durchsetzungsmechanismen

122. Gestützt auf die Kriterien in dem Referenzpapier zur Angemessenheit hat sich der EDSA mit folgenden Aspekten des japanischen Datenschutz- und Rechtsrahmens befasst, die unter den Entwurf des Angemessenheitsbeschlusses fallen: Vorhandensein und wirksame Arbeitsweise einer unabhängigen Aufsichtsbehörde; Bestehen eines Systems, das ein hohes Maß an Konformität gewährleistet, und eines Systems für den Zugang zu geeigneten Rechtsbehelfsmechanismen, die EU-Bürgern die Möglichkeit bieten, ihre Rechte wahrzunehmen und Rechtsmittel einzulegen, ohne dabei auf schwerfällige administrative und gerichtliche Rechtsbehelfe zu stoßen.

123. Ausgehend von den Parametern, die der EuGH in der Rechtssache *Schrems*[53] festgelegt hat, und von den Parametern, die in Erwägungsgrund 104 und Artikel 45 DSGVO dargelegt sind, stellt der EDSA fest, dass es in Japan zwar ein System gibt, das sich zum europäischen kohärent verhält, dass dieses System jedoch für EU-Bürger, deren Daten im Rahmen dieses Angemessenheitsbeschlusses übermittelt werden, angesichts sprachlicher und institutioneller Hindernisse in der Praxis möglicherweise nur schwer zugänglich ist.

[51] Für kritische Anmerkungen zum Konzept der Einwilligung im japanischen Datenschutzrechtsrahmen siehe: 2.1. Allgemeines und 2.2.8. Direktwerbung.

[52] Diese sektorspezifischen Vorschriften lagen dem EDSA nicht vor.

[53] Rechtssache C-362/14 (2015) Maximilian Schrems / Data Protection Commissioner (Rn. 73 und 74).

124. In den folgenden Abschnitten werden zunächst die oben genannten Aspekte des japanischen Rechtsrahmens geprüft und dann einige Empfehlungen für die Kommission formuliert.

3.2.1 Zuständige unabhängige Aufsichtsbehörde

125. Die PPC wurde am 1. Januar 2016 nach der Änderung des APPI von 2015 eingerichtet und trat an die Stelle ihrer Vorgängerin, der Sonderkommission für den Schutz personenbezogener Daten (eingerichtet 2013 nach dem „My Number Act"). Obwohl sie noch eine junge Organisation ist, hat die PPC seit ihrer Gründung erhebliche Anstrengungen unternommen, um die erforderliche Infrastruktur aufzubauen, die die Umsetzung des geänderten APPI ermöglichen soll. Zu nennen sind in diesem Zusammenhang die PPC-Vorschriften, die PPC-Leitlinien, die den PIHBO Orientierungshilfe bei der Auslegung des APPI geben sollen, die Veröffentlichung eines F&A-Dokuments der PPC[54] und die Einrichtung einer Helpline für die Beratung von Unternehmern und Bürgern über die Datenschutzbestimmungen sowie die Einrichtung eines Mediationsdienstes zur Bearbeitung von Beschwerden.

126. Einrichtung und Arbeitsweise der PPC sind in Kapitel V des APPI geregelt. Obwohl die PPC in den Zuständigkeitsbereich des Premierministers fällt, ist sie gemäß Artikel 62 in der Wahrnehmung ihrer Aufgabe unabhängig. Der EDSA begrüßt die Klarstellung der Europäischen Kommission im geänderten Entwurf des Angemessenheitsbeschlusses vom 13. November 2018 in der Frage, inwieweit die PCC frei von internen und externen Einflüssen ist.

3.2.2 Das Datenschutzsystem muss ein hohes Maß an Konformität gewährleisten

127. Der Entwurf des Angemessenheitsbeschlusses beinhaltet eine umfassende Prüfung der Befugnisse der PPC gemäß den Artikeln 40, 41 und 42 APPI zur Überwachung und Durchsetzung der Rechtsvorschriften. Artikel 40 ermächtigt die PPC, von PIHBO Berichte und Unterlagen über Verarbeitungsvorgänge anzufordern, und zur Durchführung von Prüfungen vor Ort. Gemäß Artikel 42 ist die PPC befugt – wenn es ihrer Auffassung nach notwendig ist, individuelle Rechte zu schützen, oder bei Verstößen gegen das Gesetz –, gegenüber PIHBO Empfehlungen auszusprechen und, sofern diese nicht greifen, ihnen anzuordnen, den Verstoß zu beenden oder die erforderlichen Maßnahmen zu ergreifen, um den Verstoß zu korrigieren.

128. Im Oktober 2018 hat die PPC eine ihrer ersten Maßnahmen gemäß Artikel 41 des geänderten APPI ergriffen und einen „Leitfaden" für einen PIHBO herausgegeben, in dem dem Unternehmen geraten wird, seine Sicherheitsmaßnahmen zu verstärken und die Anbieter von Anwendungen wirksam zu überwachen und den Nutzern klar und leicht verständlich zu erläutern, wie ihre personenbezogenen Daten verwendet werden, und vorab die Einwilligung einzuholen, wenn die Informationen mit einem Dritten ausgetauscht werden, sowie auf Anträge von Nutzern auf Löschung ihrer Informationen angemessen zu reagieren. In den Antworten an den EDSA[55] teilten Mitarbeiter der PPC mit, das Unternehmen habe seine Kooperationsbereitschaft bekundet, und wenn das Unternehmen dem nicht nachkomme, werde sie dem Unternehmen gegenüber eine „Empfehlung" gemäß Artikel 42 Absatz 1 APPI aussprechen.

129. Die von der PPC durchgeführte Untersuchung gegen den genannten PIHBO ist ein sehr positiver Indikator für die Bemühungen der japanischen Aufsichtsbehörde, für ein gutes Konformitätsniveau im Land zu sorgen.

130. Zwar sind einige Verbesserungen im Vergleich zu dem Rahmen festzustellen, der vor 2015 bestand, doch stellt der EDSA fest, dass die PPC weniger Befugnisse hat als europäische Datenschutzbehörden

[54] Dieses Dokument wurde dem EDSA von der Europäischen Kommission nicht in englischer Sprache vorgelegt.
[55] Anhang III.

nach der DSGVO, insbesondere in Bezug auf die **Durchsetzung**. Bußgelder[56] sind z. B. sehr niedrig. Im Durchführungsbeschluss der Europäischen Kommission heißt es in Erwägungsgrund 108, dass im Falle der Nichteinhaltung oder einiger Verstöße gegen das APPI strafrechtliche Sanktionen verhängt werden und der Vorsitzende der PPC die Fälle an die Staatsanwaltschaft weiterleiten kann. Der Beschluss der Europäischen Kommission trägt jedoch nicht der Tatsache Rechnung, dass die Strafverfolgung in Japan nach freiem Ermessen erfolgt und mitunter Gegenstand langwieriger Überprüfungsverfahren sein kann.[57] Darüber hinaus kann es schwierig sein, eine Freiheitsstrafe (mit oder ohne Arbeit) im Zusammenhang mit Verstößen gegen das APPI gemäß den Bestimmungen in Kapitel VII zu verhängen, weil sie für natürliche Personen gelten und der PIHBO als juristische Person in keinem Fall für eine Nichterfüllung seiner Rechenschaftspflicht bestraft wird

131. **Vor diesem Hintergrund fordert der EDSA die Europäische Kommission auf, die Wirksamkeit der Sanktionen und der entsprechenden Abhilfemaßnahmen im japanischen Datenschutzsystem genau zu überwachen.**

3.2.3 Das Datenschutzsystem muss betroffenen Einzelpersonen bei der Ausübung ihrer Rechte Unterstützung und Hilfe sowie angemessene Rechtsschutzverfahren bieten

132. Die PPC stellt auf ihrer Website umfangreiche Informationen und Leitlinien zur Aufklärung der PIHBO über ihre Pflichten und Verantwortlichkeiten nach dem Datenschutzrahmen sowie eine Helpline zur Information und Unterstützung japanischer Bürger im Hinblick auf ihre individuellen Rechte im Rahmen des APPI zur Verfügung. Die Website umfasst auch einen Bereich mit der Bezeichnung „Children's room" (Kinderzimmer), der sich ausdrücklich an Kinder und Jugendliche wendet. Der EDSA hält fest, dass diese Informationen ebenso wie Helpline-Unterstützung, Beratung und F&A-Dokumente in japanischer Sprache verfügbar sind.[58] Der EDSA ist daher zutiefst davon überzeugt, dass es von Nutzen wäre, wenn die PPC eine eigenständige englische Fassung ihrer Website zur Verfügung stellen würde, die EU-Bürgern, deren Daten auf der Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission nach Japan übermittelt werden, Informationen über ihre individuellen Rechte nach dem japanischen Datenschutzregelwerk und den Ergänzenden Vorschriften bietet.

133. Der EDSA begrüßt die Klarstellung durch die Europäische Kommission in Erwägungsgrund 104 des am 13. November 2018 vorgelegten geänderten Entwurfs des Angemessenheitsbeschlusses in Bezug auf den von der PPC gemäß Artikel 61 Ziffer ii APPI geleiteten Mediationsdienst. Trotzdem möchte der EDSA in diesem Zusammenhang drei Punkte ansprechen. Erstens wird der Mediationsdienst in der englischsprachigen Version der PPC-Website nicht bekannt gemacht. Zweitens kann der Dienst nur telefonisch und in japanischer Sprache in Anspruch genommen werden. Schließlich ist Mediation nur ein Vermittlungsprozess, der nicht zu einer verbindlichen Vereinbarung zwischen den Parteien führt, was sich auf die Wirksamkeit der den betroffenen Personen zur Verfügung stehenden Rechtsbehelfe auswirkt.[59]

---

[56] Sie sind in Kapitel VII des APPI aufgeführt. Die Höchststrafe ist festgelegt in Artikel 83 (Bereitstellung oder betrügerische Nutzung einer Datenbank mit personenbezogenen Daten zur Erzielung eines unrechtmäßigen Gewinns für sich selber oder einen Dritten) und entspricht einer Freiheitsstrafe von einem Jahr mit Arbeit oder einer Geldbuße von höchstens 500 000 Yen (rund 3 900 EUR). Nach den Erläuterungen der Kommission werden Geldbußen pro Verstoß kumulativ verhängt. Auch wenn dies zutreffen mag, stellt der EDSA fest, dass selbst bei der Verhängung kumulativer Geldbußen der Gesamtbetrag im Vergleich zu europäischen Standards vermutlich deutlich niedriger ausfallen dürfte.

[65] Oda H., Japanese Law, Oxford University Press (III edition), 2009: 439 – 440.

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; and Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (ed.).

134. Im Übrigen stellt der EDSA fest, dass der Entwurf eines Angemessenheitsbeschlusses den Schwerpunkt auf die im Wege des Zivilrechts und des Strafverfahrens verfügbaren Rechtsbehelfe legt, jedoch nicht einräumt, dass es **institutionelle Hindernisse für Rechtsstreitigkeiten** in Japan gibt, wie z. B. Gerichtskosten (die Gerichtskosten sind zu gleichen Teilen von Kläger und Beklagtem zu tragen, unabhängig davon, welche Partei obsiegt[60]), der Mangel an Anwälten in dem Land[61], die Tatsache, dass ausländische Rechtsanwälte nicht nach inländischem Recht tätig werden dürfen, sowie die Beweislast im Schadensersatzrecht. Der EDSA befürchtet, dass diese Faktoren den Zugang der Bürger zur Justiz in der Praxis behindern und ihr Recht gefährden könnten, rasch und ohne überhöhte Kosten Rechtsmittel einzulegen.

135. Vor diesem Hintergrund **hegt der EDSA wegen des Risikos Bedenken, dass EU-Bürger Schwierigkeiten beim Zugang zu behördlichem und gerichtlichem Rechtsschutz haben könnten** und würde es daher begrüßen, wenn die Europäische Kommission mit der PPC die Möglichkeit erörtern würde, zumindest in englischer Sprache einen Online-Dienst einzurichten, der **EU-Bürger unterstützt und ihre Beschwerden[62] bearbeitet**. Darüber hinaus würde es der EDSA begrüßen, wenn EU-Datenschutzbehörden die Möglichkeit gegeben würde, im Falle von Beschwerden bei in Japan tätigen Organisationen und der PPC für betroffene Personen aus der EU als zwischengeschaltete Stelle tätig zu werden.

4 ÜBER DEN ZUGANG VON BEHÖRDEN ZU DEN NACH JAPAN ÜBERMITTELTEN DATEN

136. Die Kommission will mit dem Angemessenheitsbeschluss anerkennen, dass „Japan ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die aus der Europäischen Union an Betreiber von Unternehmen für die Verarbeitung personenbezogener Daten in Japan übermittelt werden“, wie es in Artikel 1 des Entwurfs des Angemessenheitsbeschlusses heißt. Im Einklang mit Artikel 45 Absatz 2 DSGVO hat die Kommission auch die Beschränkungen und Garantien für den Zugang von Behörden zu personenbezogenen Daten analysiert. Der Schwerpunkt in diesem Kapitel liegt auf der Prüfung des Zugangs von Strafverfolgungsbehörden und anderen staatlichen Stellen zu personenbezogenen Daten für Zwecke der nationalen Sicherheit. Grundlage für die Analyse des EDSA ist Anhang II des Entwurfs des Angemessenheitsbeschlusses, in dem die japanische Regierung einen Überblick über den einschlägigen Rechtsrahmen und die japanischen Rechtsvorschriften gibt, soweit diese von der Kommission zur Verfügung gestellt wurden. Im spezifischen Kontext dieser Prüfung hat der EDSA daher Elemente japanischer Gesetze berücksichtigt, die nicht Teil der Feststellungen der Europäischen Kommission sind, aber doch für die Beurteilung der Bedingungen und Garantien relevant sind, unter denen japanische Behörden auf aus der Europäischen Union übermittelte personenbezogene Daten zugreifen dürfen.

[60] Wagatsuma (2012), ‘Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure’ in Reimann (ed.), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice Vol. 11, pp. 195 – 200.

[61] Nach den jüngsten Zahlen gibt es in Japan 38 980 Rechtsanwälte (ungefähr 290 Anwälte auf eine Million Einwohner) [Japan Federation of Bar Association] (2017), White Paper on Attorneys: p. 8 – 9.

[62] Ähnlich der in Anhang II dieses Angemessenheitsbeschlusses für Beschwerden von EU-Bürgern bezüglich des Zugangs japanischer Behörden zu ihren Daten vorgesehenen.

4.1 Zugang zu Daten für Strafverfolgungsbehörden

4.1.1 Verfahren für den Zugang zu Daten im Bereich des Strafrechts

137. In dem Entwurf des Angemessenheitsbeschlusses werden drei Verfahren vorgestellt, die es nach japanischem Recht für Strafverfolgungsbehörden für den Zugang zu Daten in Japan gibt:

4.1.1.1 Anträge auf Zugang mit einer richterlichen Anordnung

138. In dem Entwurf des Angemessenheitsbeschlusses heißt es, dass in Japan öffentliche Stellen und insbesondere Strafverfolgungsbehörden, die im Rahmen strafrechtlicher Ermittlungen auf elektronische Beweismittel zugreifen möchten, hierfür stets eine Anordnung benötigen, sofern sie nicht das Verfahren der freiwilligen Offenlegung anwenden – siehe weiter unten.

4.1.1.1.1 Erfordernis einer „angemessenen Ursache", Notwendigkeit und Verhältnismäßigkeit der Anordnungen

139. Der EDSA stellt fest, dass gemäß der japanischen Verfassung für jede Erhebung personenbezogener Daten mit Zwangsmitteln eine gerichtliche Anordnung vorliegen muss. Im Entwurf des Angemessenheitsbeschlusses wird insbesondere darauf hingewiesen, dass in allen Fällen von „Durchsuchungen und Beschlagnahmen" gerichtliche Anordnungen für eine „angemessene Ursache" zu erlassen sind, die nach Auffassung des Obersten Gerichtshofs nur dann vorliegt, wenn davon auszugehen ist, dass die betreffende Person (Verdächtiger oder Beschuldigter) eine Straftat begangen hat und die Durchsuchung und Beschlagnahme für die strafrechtlichen Ermittlungen erforderlich ist. Die Kommission verweist hier auf das Urteil des Obersten Gerichtshofs vom 18. März 1969 in der Rechtssache N. 100 (1968(Shi)). Der EDSA weist darauf hin, dass nach der Rechtsprechung des EuGH[63] nur ein Gericht, und nicht beispielsweise ein Staatsanwalt, die Erhebung insbesondere von Verkehrs- und Standortdaten genehmigen kann.

140. Auch vor dem Hintergrund der Rechtsprechung des EuGH, der zufolge der Zugriff auf Daten Gegenstand einer Anordnung sein kann, wie in Tele2, bedauert der EDSA, dass keine zusätzlichen Informationen zur Prüfung der Frage zur Verfügung gestellt wurden, wie die Kriterien für die Beurteilung der Notwendigkeit einer Anordnung – Schwere der Straftat, Art und Weise der Begehung der Straftat, Wert und Bedeutung des beschlagnahmten Materials als Beweismittel, Wahrscheinlichkeit des Verbergens oder der Vernichtung beschlagnahmten Materials, Umfang der durch eine Beschlagnahme verursachten Nachteile, andere damit zusammenhängende Bedingungen – und das aus der Verfassung abgeleitete Konzept der angemessenen Ursache in der Praxis angewandt werden. Daher fordert der EDSA die Kommission auf, zu überwachen, ob der Erlass von Anordnungen in der Praxis die vom EuGH festgelegten Kriterien erfüllt.

4.1.1.1.2 Arten von Straftaten, bei denen Anordnungen erlassen werden können

141. Das Anordnungsverfahren findet nur Anwendung, wenn eine „obligatorische Untersuchung" durchgeführt wird. Diese Anordnungen können grundsätzlich nur in Fällen erlassen werden, in denen ein Verstoß gegen das Gesetz vorliegt. In diesem Zusammenhang nimmt der EDSA das kürzlich verabschiedete „Gesetz über die Bestrafung organisierter Kriminalität und die Kontrolle von Erträgen aus Straftaten" zur Kenntnis, das am 15. Juni 2017 im Zusammenhang mit dem Beitritt Japans zum Internationalen Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende Kriminalität (UNTOC)[64] angenommen wurde. In Ermangelung einer verfügbaren englischen Fassung dieser Rechtsvorschriften und angesichts der unionsrechtlichen Vorgabe, dass einige Daten nur im Zusammenhang mit der Ermittlung, Feststellung oder Verfolgung von schweren Straftaten erhoben

[63] Siehe die Rechtssachen C-203/15, C-293/12 und C-594/12 des EuGH.
[64] Siehe: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .

werden[65], sowie angesichts der von mehreren Kommentatoren, darunter dem Sonderberichterstatter der Vereinten Nationen Joseph Cannataci[66], geäußerten Bedenken bezüglich des breiten Anwendungsbereichs, der sich auf eine angeblich vage und zu weit gefasste Definition des Begriffs „organisierte kriminelle Gruppe“ stützt, kann der EDSA nicht zu dem Schluss gelangen, dass der Zugang zu elektronischen Beweismitteln nach den einschlägigen japanischen Rechtsvorschriften auf die im EU-Recht vorgesehenen Schwellenwerte beschränkt ist.

142. Es sei auch darauf hingewiesen, dass für manche Arten von Straftaten die Präfekturpolizei zuständig ist und dass diese ihre eigenen Polizeiverordnungen hat. Die für die Präfekturpolizei geltenden internen Vorschriften lagen dem EDSA nicht vor.

143. Dem Entwurf der Angemessenheitsentscheidung zufolge fällt die Erhebung elektronischer Informationen im Bereich Strafverfolgung in die Zuständigkeit der Präfekturpolizei.

4.1.1.2 Anordnungen über das Abhören des Telefonverkehrs

144. In Anhang II des Entwurfs des Angemessenheitsbeschlusses wird darauf hingewiesen, dass das Gesetz über das Abhören des Telefonverkehrs im strafrechtlichen Ermittlungsverfahren Besonderheiten bei der Überwachung des Fernmeldeverkehrs vorsieht. Diese Rechtsvorschriften wurden sehr spät vorgelegt, so dass eine eingehende Analyse nicht möglich war. Auch wenn dieser Rechtsrahmen anscheinend viele Garantien bietet, ist der EDSA nicht in der Lage, zu beurteilen, ob die in diesem Rechtsakt vorgesehenen Bedingungen mit Garantien verbunden sind, die im Wesentlichen den in der EU sowohl durch die Charta in der Auslegung durch den EuGH als auch durch die EMRK in der Auslegung durch den Gerichtshof in Straßburg gebotenen Garantien gleichwertig sind.

4.1.1.3 Das Verfahren der „freiwilligen Offenlegung“ auf der Grundlage eines Auskunftsformulars

145. Diese nicht obligatorische Form der Zusammenarbeit ermöglicht es Behörden, für die Verarbeitung Verantwortliche (mit Ausnahme von Telekommunikationsbetreibern) um die Übermittlung von Daten zu bitten. Ein Nicht-Eingehen auf die Anfrage kann nicht durchgesetzt werden. Es bleibt unklar, welche Behörden diese Art von Verfahren verwenden können, aber es scheint auf Strafverfolgungsbehörden beschränkt zu sein.

4.1.1.3.1 Voraussetzungen für die Ausstellung von „Auskunftsformularen“

146. Der EDSA erkennt an, dass der Oberste Gerichtshof Japans unter Verweis auf die Verfassung Grenzen für die Verwendung „freiwilliger Offenlegungen“ abgesteckt hat.[67] Aus dem Entwurf des Angemessenheitsbeschlusses geht hervor, dass konkret eine „freiwillige Offenlegung“ nur im Wege der Ausstellung eines „Auskunftsformulars“ durch die zuständigen Behörden verlangt werden kann. Die Übermittlung eines solchen „Auskunftsformulars“ ist offenbar nur im Rahmen einer strafrechtlichen Ermittlung zulässig und setzt somit immer einen konkreten Verdacht auf eine bereits begangene Straftat voraus. Solche Ermittlungen werden in der Regel von der Präfekturpolizei durchgeführt, für die die Beschränkungen gemäß Artikel 2 Absatz 2 des Polizeigesetzes gelten, was bedeutet, dass sie für die Polizeiarbeit von Belang sein sollten. Der EDSA benötigt jedoch weitere Präzisierungen bezüglich der konkreten Gestaltung der Kriterien, die das Ausstellen eines Auskunftsformulars ermöglichen (wie z. B. Rechtsprechung zur Illustration der Anwendung dieser Kriterien), sowie zur Beziehung zwischen dem Verfahren der freiwilligen Offenlegung und der Beschlagnahme von Daten auf der Grundlage einer Anordnung. Es zeigt sich nämlich, dass, selbst wenn

[65] Siehe verbundene Rechtssachen C-293/12 und C-594/12 sowie Rechtssache C-203/15.
[66] Sonderberichterstatter der Vereinten Nationen für das Recht auf Privatsphäre sowie Graham Greenleaf, UNSW Law Researcher.
[67] Siehe Anhang II, S. 8.

Daten im Rahmen des freiwilligen Verfahrens nicht beschafft werden könnten, sie immer noch mit einer Anordnung erlangt werden könnten, wenn dies für die Ermittlungsbehörden unerlässlich ist.[68]

4.1.1.3.2 Verfügbare Rechtsprechung zu den Grenzen der Verwendung der freiwilligen Offenlegung

147. Die im Entwurf des Angemessenheitsbeschlusses zitierten Fälle[69], mit denen die Anwendung des Verfahrens der freiwilligen Offenlegung illustriert werden soll, sind Fälle, in denen die beschuldigte Person im öffentlichen Raum direkt von der Polizei entweder fotografiert oder gefilmt wurde, und sie geben daher nur begrenzt Hinweise auf Situationen, in denen die zuständigen Behörden einen für die Verarbeitung Verantwortlichen um die Offenlegung von Daten ersuchen können, insbesondere im Hinblick auf die in Anhang II aufgeführten Kriterien der „Angemessenheit der Methoden", was die Beurteilung zu betreffen scheint, ob freiwillige Ermittlungen „angemessen" oder vernünftig sind, um den Zweck der Ermittlung zu erreichen. Gleiches gilt für das allgemeine Kriterium, „ob sie im Einklang mit gesellschaftlich akzeptierten Konventionen als angemessen angesehen werden können", um die Rechtmäßigkeit freiwilliger Ermittlungen zu bewerten. Darüber hinaus hat die Nationale Polizeibehörde als die für alle Angelegenheiten im Zusammenhang mit der Kriminalpolizei zuständige Bundesbehörde der Präfekturpolizei Weisungen in Bezug auf die „ordnungsgemäße Verwendung schriftlicher Anfragen in Ermittlungsangelegenheiten" erteilt. Unter anderem muss der Hauptermittler intern die Genehmigung eines hochrangigen Beamten einholen. Dem EDSA liegen keinerlei Informationen dazu vor, ob diese Weisungen verbindlich sind. Allerdings hält der EDSA fest, dass die Anwendung dieses Verfahrens verhältnismäßig oder notwendig sein muss.

4.1.1.3.3 Rechte und Pflichten der für die Verarbeitung Verantwortlichen im Rahmen der freiwilligen Offenlegung

148. Darüber hinaus ist es Sache der für die Verarbeitung Verantwortlichen, der Bereitstellung von Daten zuzustimmen (es besteht jedoch offenbar keine Verpflichtung, die Einwilligung der betroffenen Personen einzuholen oder sie zu informieren), wenn diese Ersuchen nicht im Widerspruch zu anderen rechtlichen Verpflichtungen (z. B. Verpflichtung zur Wahrung der Vertraulichkeit) stehen. Aus dem Bericht der Kommission geht hervor, dass die für die Verarbeitung Verantwortlichen nach einer anfänglich hohen Antwortquote nunmehr damit begonnen haben, an den Datenschutz ihrer Kunden zu denken und somit weniger häufig auf diese Anfragen eingehen.

149. Es bleibt auch unklar, ob für die für die Verarbeitung Verantwortlichen ein Anreiz besteht, der Anfrage nachzukommen (ob z. B. ein Nachkommen einen Vorteil für sie bedeutet oder ob sie strafrechtlich nicht verfolgt werden usw.). Insbesondere wird kein Grundsatz wie derjenige erwähnt, dass die Aussage verweigert werden kann, wenn die Befürchtung besteht, sich selbst zu belasten.

150. Der EDSA würde, soweit verfügbar, zusätzliche Informationen über Anzahl und Art der Anfragen sowie die von den für die Verarbeitung Verantwortlichen übermittelten Antworten begrüßen. In Ermangelung von Rechtsprechung und Zahlen fordert der EDSA die Kommission auf, die Effizienz und die konkrete Anwendung dieses Verfahrens in der Praxis zu überwachen.

151. Um sich zu diesen Elementen äußern zu können, fehlt es dem EDSA jedoch an Rechtsprechung und Zahlen. Folglich ist der EDSA nicht in der Lage, ohne nähere Angaben zur Praxis die Effizienz und konkrete Anwendung dieses Verfahrens zu bewerten.

[68] Siehe Anhang II, S. 7.
[69] Siehe Anhang II, S. 8 – zwei Urteile des Obersten Gerichtshofs vom 24. Dezember 1969, (1965 (A) Nr. 1187) bzw. 15. April 2008 (2007 (A) Nr. 839).

4.1.1.4 Schlussfolgerung zu den Verfahren für den Zugang zu Daten zu Strafverfolgungszwecken

152. Zusammenfassend erkennt der EDSA an, dass der Grundsatz, nach dem personenbezogene Daten den zuständigen Behörden nur dann mit Zwangsmitteln zugänglich gemacht werden dürfen, wenn dies für den Zweck erforderlich und verhältnismäßig ist und es auf der Grundlage einer Anordnung geschieht, die den wichtigsten wesentlichen Garantien entspricht, die nach dem EU-Recht und der Rechtsprechung des EGMR geboten sind. Im Lichte dieser Feststellungen fordert der EDSA die Kommission auf, den Anwendungsbereich dieser Maßnahmen, den Anwendungsbereich des Verfahrens der freiwilligen Offenlegung und die Anwendung dieses Grundsatzes durch die Präfekturpolizei und die Gerichte in der einschlägigen Rechtsprechung zu überwachen und auch zu überwachen, ob der japanische Rechtsrahmen die wesentlichen Garantien bietet, die der EuGH auf der Grundlage der Charta und der EGMR auf der Grundlage des Übereinkommens formuliert hat.

4.1.2 Aufsicht im Bereich des Strafrechts

153. In dem Entwurf des Angemessenheitsbeschlusses und in dessen Anhang II werden vier Arten von Aufsichtsformen über Polizei, Ministerien und öffentliche Stellen vorgestellt.

4.1.2.1 Gerichtliche Aufsicht

4.1.2.1.1 In Fällen, in denen elektronische Daten mit Zwangsmitteln (Durchsuchung und Beschlagnahme) erhoben werden

154. Gemäß dem Entwurf des Angemessenheitsbeschlusses muss die Polizei in allen Fällen, in denen elektronische Daten mit Zwangsmitteln (Durchsuchung und Beschlagnahme) erhoben werden, eine vorherige richterliche Anordnung erwirken. Es gibt jedoch eine Ausnahme von dieser Regel.[70] In Artikel 220 Absatz 1 der Strafprozessordnung ist nämlich vorgesehen, dass ein Staatsanwalt, sein Assistent oder ein Kriminalbeamter bei der Verhaftung eines Verdächtigen elektronische Informationen am Ort der Festnahme durchsuchen oder beschlagnahmen darf. In einem solchen Fall besteht die Möglichkeit, dass solche Informationen von einem Richter als Beweismittel ausgeschlossen werden.

155. Der EDSA ist sich der Tatsache bewusst, dass ähnliche Ausnahmen auch im EU-Recht vorgesehen sind. Er stellt fest, dass in Fällen, in denen elektronische Informationen mit Zwangsmitteln erhoben werden, nicht immer eine gerichtliche Kontrolle gegeben ist, wie im Entwurf des Angemessenheitsbeschlusses vorgesehen. In diesem Zusammenhang verweist der EDSA auf die Rechtsprechung des EGMR in Bezug auf gerichtliche Nachprüfungen.[71]

4.1.2.1.2 Im Falle von Ersuchen um freiwillige Offenlegung

156. Gemäß dem Entwurf des Angemessenheitsbeschlusses gibt es bei Ersuchen um freiwillige Offenlegung keine Ex-ante-Kontrolle durch einen Richter. In diesem Fall wird die Präfekturpolizei unter der Aufsicht durch die Staatsanwaltschaft tätig. Im Entwurf des Angemessenheitsbeschlusses werden Artikel 192 Absatz 1 und Artikel 246 über die Zusammenarbeit und Koordinierung von Staatsanwaltschaft, Kommissionen für öffentliche Sicherheit der Präfekturen und Kriminalpolizei sowie der Informationsaustausch zwischen ihnen erwähnt. Verwiesen wird ferner auf Artikel 193 Absatz 1, wonach die Staatsanwaltschaft erforderlichenfalls Weisung an die Kriminalpolizei erteilen und Standards für eine faire Ermittlung festlegen kann. Im Übrigen wird Artikel 194 über Disziplinarmaßnahmen gegen die Kriminalpolizei wegen Missachtung der Staatsanwaltschaften erwähnt, die von den Kommissionen für öffentliche Sicherheit auf nationaler Ebene oder in den Präfekturen verhängt werden.

[70] Siehe Anhang II.
[71] EGMR, Modestou gegen Griechenland, Nr. 51693/13.

157. Der EDSA nimmt Kenntnis von der Einführung der bisherigen Maßnahmen und der Aufsicht über die Kriminalpolizei durch die Kommissionen für öffentliche Sicherheit auf nationaler Ebene und in den Präfekturen (siehe weiter unten).

4.1.2.2 Aufsicht über die Polizei durch die Kommissionen für öffentliche Sicherheit

158. Gemäß Anhang II des Entwurfs des Angemessenheitsbeschlusses üben zwei Arten von Kommissionen die Aufsicht über die Polizei aus. Beide heben auf die Sicherung des demokratischen Managements und der politischen Neutralität der Polizeiverwaltung ab.

4.1.2.2.1 Aufsicht durch die Nationale Kommission für öffentliche Sicherheit

159. In Anhang II des Entwurfs des Angemessenheitsbeschlusses wird die Aufsicht über die nationale Polizeiverwaltung (NPA) durch die Nationale Kommission für öffentliche Sicherheit erwähnt. Das Polizeigesetz enthält eine Liste der Aufgaben der Kommission, aus der ihre Aufsichtsbefugnis hervorgeht (siehe Artikel 5).

160. Gemäß Artikel 4 des Polizeigesetzes gehört die Nationale Kommission für öffentliche Sicherheit zum Zuständigkeitsbereich des Ministerpräsidenten und besteht aus einem Vorsitzenden und fünf Mitgliedern. Artikel 7 sieht einige Beschränkungen bei der Ernennung der Mitglieder der Kommission vor. Die Amtszeit der Mitglieder der Kommission beträgt fünf Jahre und kann nach Artikel 8 nur einmal verlängert werden. Darüber hinaus scheint das Parlament über eine starke Macht hinsichtlich der Ernennung und Entlassung der Mitglieder der Kommission zu verfügen, was die Unabhängigkeit der Nationalen Kommission für öffentliche Sicherheit gewährleistet.

161. Durch solche Rechtsvorschriften wird die politische Neutralität der Nationalen Kommission für öffentliche Sicherheit gestärkt.

4.1.2.2.2 Aufsicht durch Präfekturkommissionen für öffentliche Sicherheit

162. Die Präfekturpolizei unterliegt der Aufsicht durch die in jeder Präfektur eingerichteten Präfekturkommission für öffentliche Sicherheit. Gemäß Artikel 2 und Artikel 36 Absatz 2 des Polizeigesetzes sind die Präfekturkommissionen für öffentliche Sicherheit für den „Schutz der Rechte und der Freiheiten einer Person“ zuständig. In Artikel 38 sowie Artikel 42 des Polizeigesetzes sind die Aufgaben der Präfekturkommissionen für öffentliche Sicherheit aufgeführt. Auch diese Kommissionen sollen das demokratische Management und die politische Neutralität der Polizeiverwaltung gewährleisten, wie in Artikel 43 Absatz 2 vorgesehen, indem sie bei der Präfekturpolizei Einzelfällen nachgehen, wenn sie dies im Rahmen einer Kontrolle der Tätigkeiten der Präfekturpolizei oder bei Feststellung eines Fehlverhaltens ihres Personals für erforderlich halten.

163. Es ist jedoch unklar, ob diese Kommissionen über andere Befugnisse verfügen als zur Überprüfung des Verhaltens der Polizei. Der EDSA stellt sich die Frage, ob der Begriff „Fehlverhalten“ den rechtswidrigen Zugriff auf Daten umfasst und ob diese Kommissionen in einem solchen Fall in der Lage sind, die Löschung von Daten anzuordnen.

164. Zur Neutralität und Unabhängigkeit dieser Kommissionen ist anzumerken, dass, wie es im Entwurf des Angemessenheitsbeschlusses heißt[72], die Präfekturkommissionen für öffentliche Sicherheit im Zuständigkeitsbereich des Gouverneurs der Präfektur eingerichtet werden, der die Mitglieder der Kommission mit Zustimmung der Präfekturversammlung zu ernennen hat. Die Amtszeit der Mitglieder der Präfekturkommission für öffentliche Sicherheit beträgt drei Jahre; sie können höchstens zweimal wiederernannt werden. Artikel 39 des Polizeigesetzes sieht Einschränkungen bei der Ernennung der Mitglieder vor. In dem Entwurf des Angemessenheitsbeschlusses wird ferner unter Verweis auf

[72] Siehe Entwurf des Angemessenheitsbeschlusses, S. 31.

Artikel 100 des Gesetzes über die örtliche Selbstverwaltung erwähnt, dass eine Aufsicht über die Präfekturpolizei durch lokale Versammlungen erfolgt. Dieser Rechtsakt wurde dem EDSA jedoch nicht vorgelegt.[73]

165. Darüber hinaus gilt gemäß Artikel 42 Absatz 2 und 3 des Polizeigesetzes Folgendes: „Ein Mitglied der Kommission kann nicht gleichzeitig Mitglied der Versammlung oder des Vollzeitpersonals lokaler öffentlicher Einrichtungen sein oder in Teilzeit tätig sein, wie in Ziffer 1 von Artikel 28 Absatz 5 des Gesetzes über den lokalen öffentlichen Dienst vorgeschrieben."

166. Im Lichte der vorstehenden Ausführungen und unter Berücksichtigung der Zusammenarbeit zwischen den Präfekturkommissionen für öffentliche Sicherheit und der Nationalen Kommission für öffentliche Sicherheit ist der EDSA mit dem Entwurf des Angemessenheitsbeschlusses einverstanden und begrüßt die Neutralität und Unabhängigkeit der Mitglieder der Präfekturkommissionen für öffentliche Sicherheit. Der EDSA geht davon aus, dass Präfekturkommissionen lediglich befugt sind, das Verhalten der Polizei zu untersuchen, und keine sonstigen Aufsichtsbefugnisse haben, einschließlich der Löschung von Daten, die von der Präfekturpolizei erhoben wurden. Es besteht daher Klärungsbedarf bezüglich der Frage, ob die von Präfekturkommissionen für öffentliche Sicherheit ausgeübte Aufsicht nach den im EU-Recht festgelegten Standards ausreichend ist.

4.1.2.2.3 Aufsicht durch das Parlament

167. Der Entwurf des Angemessenheitsbeschlusses[74] und Anhang II[75] enthalten einige Informationen über die Aufsicht, die das Parlament über die Regierung ausübt, auch im Hinblick auf die Rechtmäßigkeit der Erhebung von Daten durch die Polizei. So wird in beiden auf Artikel 62 der Verfassung verwiesen, wonach das Parlament die Vorlage von Dokumenten und Zeugenaussagen verlangen kann. Beide sprechen auch Bestimmungen des japanischen Parlamentsgesetzes an, insbesondere Artikel 104 über die Befugnisse des japanischen Parlaments sowie Artikel 74 über die Einreichung schriftlicher Anfragen, die gemäß Artikel 75 binnen sieben Tagen schriftlich vom Kabinett zu beantworten sind. Im Entwurf des Angemessenheitsbeschlusses wird noch hinzugefügt: „Die Rolle des japanischen Parlaments bei der Aufsicht über die Exekutive wird gestützt durch Berichtspflichten, z. B. gemäß Artikel 29 des Gesetzes über das Abhören des Telefonverkehrs".

168. Der Europäische Datenschutzausschuss erkennt die Beteiligung des Parlaments an der Kontrolle der Regierung und der Polizei in Bezug auf die Rechtmäßigkeit der Datenerhebung an.

4.1.2.2.4 Aufsicht durch die Exekutive

169. Gemäß Anhang II des Entwurfs der Angemessenheit ist einerseits der Minister bzw. der Leiter jedes Ministeriums oder jeder Agentur auf der Grundlage des APPIHAO[76] für Aufsicht und Durchsetzung zuständig. Andererseits verfügt der Minister für innere Angelegenheiten und Kommunikation (MIC) über Untersuchungsbefugnisse zur Durchsetzung des APPIHAO durch alle anderen Ministerien, darunter das Justizministerium für die Polizei, wie im Entwurf des Angemessenheitsbeschlusses erwähnt.[77]

170. Der Minister kann auf der Grundlage von Artikel 50 APPIHAO den Leiter eines Verwaltungsorgans auffordern, Material und Erklärungen über den Umgang mit personenbezogenen Daten durch das betreffende Verwaltungsorgan vorzulegen. Er kann gemäß Artikel 50 und 51 APPIHAO eine

[73] Siehe Entwurf des Angemessenheitsbeschlusses, S. 33.
[74] Siehe Entwurf des Angemessenheitsbeschlusses, S. 30.
[75] Siehe Anhang II, S. 12.
[76] Siehe Anhang II, S. 10.
[77] Siehe Anhang II, S. 11.

Überprüfung der Maßnahmen verlangen, wenn der Verdacht besteht, dass ein Gesetzesverstoß oder eine unangemessene Anwendung des Gesetzes stattgefunden hat, und er kann Stellungnahmen zum Umgang mit personenbezogenen Informationen durch die betreffende Verwaltungsstelle abgeben.

171. Im Entwurf des Angemessenheitsbeschlusses und im Anhang II heißt es ferner, dass gemäß Artikel 47 APPIHAO 51 umfassende Informationszentren eingerichtet wurden, die die reibungslose Umsetzung dieses Gesetzes gewährleisten. Der EDSA stellt fest, dass Rolle und Befugnisse dieser Informationszentren im APPIHAO nicht weiter erklärt werden, dass der Entwurf des Angemessenheitsbeschlusses jedoch einige nähere Angaben enthält.

172. Daher begrüßt der EDSA die Tatsache, dass die Einhaltung des APPIHAO durch Ministerien und Verwaltungsorgane durch die Exekutive in Gestalt des MIC beaufsichtigt wird.

173. Schlussfolgerung: In den EU-Rechtsvorschriften und in der EMRK bzw. in der Rechtsprechung ihrer jeweiligen Gerichte sind Standards und Garantien festgelegt, denen zufolge die Aufsicht vollständig, neutral und unabhängig sein muss. Der EDSA hält fest, dass die PPC nicht über Aufsichtsbefugnisse im Bereich der Strafverfolgung verfügt. Darüber hinaus ist anzumerken, dass zwar die Aufsicht durch das Parlament, die Nationale Kommission für öffentliche Sicherheit und die Präfekturkommissionen für öffentliche Sicherheit neutral und unabhängig zu sein scheint, dass aber noch weitere Klarstellungen zu den Aufsichtsbefugnissen der Präfekturkommissionen für öffentliche Sicherheit erforderlich sind.

4.1.3 Rechtsbehelfe im Bereich des Strafrechts

174. Der Entwurf des Angemessenheitsbeschlusses, ergänzt durch Anhang II, bietet mehrere Wege, über die Einzelpersonen Beschwerden einreichen können, und zwar sowohl vor unabhängigen Behörden als auch bei Gericht.

175. Nachstehend wird zunächst ein kurzer Überblick über die verfügbaren Rechte gegeben, um abzuklären, was betroffene Personen von den Behörden im Zusammenhang mit der Datenverarbeitung im Bereich von Strafverfahren erwarten können, und im Anschluss wird, gestützt auf die verfügbaren Unterlagen, auf diese Wege und die Kernelemente dieser Verfahren eingegangen.

4.1.3.1 Betroffenen Personen im Zusammenhang mit Strafverfahren zur Verfügung stehende Rechte

176. Um Wiedergutmachung zu erhalten, müssen betroffene Personen nach dem Gesetz Rechte haben, damit sie ihre Ansprüche wegen nicht gewahrter Rechte geltend machen können. Daher hat der EDSA auch die im Entwurf des Angemessenheitsbeschlusses im Zusammenhang mit Strafverfahren genannten verfügbaren Rechte geprüft.

4.1.3.1.1 Allgemeine Beschränkungen der Rechte betroffener Personen nach dem APPIHAO

177. In ihrem Entwurf des Angemessenheitsbeschlusses bezieht sich die Kommission auf allgemeine Datenschutzgrundsätze, die von Behörden eingehalten werden müssen, wenn sie personenbezogene Daten erhoben haben. Diese Grundsätze werden auch in Anhang II näher erläutert, so dass der EDSA beschlossen hat, auch hierzu Stellung zu nehmen.

178. Im Hinblick auf die verfügbaren Rechte stellt der EDSA fest, dass gemäß Anhang II des Entwurfs des Angemessenheitsbeschlusses einige der allgemeinen Rechte für betroffene Personen, die im Zusammenhang mit von Verwaltungsorganen verarbeiteten Daten gewährt werden, auch im Zusammenhang mit strafrechtlichen Ermittlungen verfügbar bleiben. Allerdings ergeben sich auch aus dem APPIHAO selbst weitere Beschränkungen bezüglich der Erhebung und Verarbeitung personenbezogener Daten in diesem Zusammenhang.

179. Diese Beschränkungen, die anscheinend im Zusammenhang mit Daten gelten, die auf der Grundlage sowohl einer Anordnung als auch eines Auskunftsformulars im Rahmen der freiwilligen Offenlegung erhoben wurden, werfen Fragen zu mehreren Aspekten auf.

180. Was den Grundsatz der Zweckbindung betrifft, müssen die Verwaltungsorgane zwar grundsätzlich den Zweck angeben, für den sie personenbezogene Daten speichern, und sie dürfen sie nicht über den für die Erfüllung der festgelegten Zweckbestimmung erforderlichen Umfang hinaus speichern, doch können sie den Zweck ändern, wenn dies als „vernünftigerweise als für den ursprünglichen Zweck angemessen angesehen werden kann".

181. Das APPIHAO sieht ebenfalls den Grundsatz der Nichtoffenlegung vor, nach dem ein Beschäftigter die erworbenen personenbezogenen Daten nicht ohne vertretbaren Grund an eine andere Person weitergeben oder für einen ungerechtfertigten Zweck nutzen darf. Es werden jedoch keine näheren Angaben zur Auslegung der Begriffe „vertretbarer Grund" und „ungerechtfertigter Zweck" gemacht, so dass hier ohne weitere Klarstellungen keine Bewertung vorgenommen werden kann.

182. In Artikel 8 Absatz 1 APPIHAO ist das Verbot geregelt, Daten zu verwenden oder offenzulegen, „sofern in den Gesetzen und sonstigen Vorschriften nichts anderes bestimmt ist". Obwohl diese Bestimmung zwar grundsätzlich nicht gegen das im EU-Recht gebotene Schutzniveau verstößt, fehlt es dem EDSA doch an näheren Informationen darüber, in welchem Umfang eine Überwachung oder Kontrolle ausgeübt wird, wenn die Offenlegung im Gesetz oder in sonstigen Vorschriften vorgesehen ist. Darüber hinaus gelten gemäß Artikel 8 Absatz 2 zusätzliche Ausnahmen von dieser Regel, wenn „durch eine solche außergewöhnliche Offenlegung die Rechte und Interessen der betroffenen Person oder eines Dritten wahrscheinlich nicht ungerechtfertigterweise beschädigt werden". Ohne weitere Informationen zu diesem Punkt bedarf diese Ausnahme, die auf dem unklaren Begriff des „ungerechtfertigten" Schadens beruht, weiter der Klärung, ob sie eng genug gefasst ist.

183. Schließlich sieht Artikel 9 APPIHAO weitere Beschränkungen beim Zweck oder der Verwendungsmethode oder sonstige Beschränkungen vor, die vom Leiter eines Verwaltungsorgans verhängt werden können, wenn gespeicherte personenbezogene Daten einer anderen Person zur Verfügung gestellt werden. Da die Begriffe „sonstige notwendige Einschränkungen" und „Bereitstellung für eine andere Person" sehr weit gefasst sind, geben diese zusätzlichen Einschränkungen der Rechte der betroffenen Person Anlass zu Bedenken, sofern nicht weitere Klarstellungen zum Geltungsbereich dieser Bestimmung erfolgen.

184. Der EDSA ist sich voll und ganz der Tatsache bewusst, dass Zugangsrechte und andere Datenschutzgrundsätze auch in Strafverfahren nach dem EU-Recht beschränkt sind, doch bestehen zusätzliche Garantien, wenn solche Beschränkungen vorgesehen sind, darunter in Bezug auf Aufsicht, Kontrolle und Rechtsbehelfe. Da es an ausreichender Rechtsprechung zu diesen Beschränkungen oder näheren Informationen zur Klarstellung des Anwendungsbereichs dieser Bestimmungen mangelt, ist der EDSA nicht in der Lage zu beurteilen, ob diese Beschränkungen der Rechte der betroffenen Person auf das begrenzt sind, was nach EU-Recht als unbedingt notwendig und verhältnismäßig gilt und somit im Wesentlichen den Rechten entspricht, die betroffenen Personen in der EU zustehen.

4.1.3.1.2 Zusätzliche Einschränkungen der Rechte im APPIHAO aufgrund der Strafprozessordnung und der Verordnungen der Präfekturpolizei

185. Der EDSA hält fest, dass das APPIHAO anscheinend auf alle Verarbeitungen durch Verwaltungsorgane in Japan Anwendung findet, dass jedoch einige wichtige Beschränkungen der Rechte der betroffenen Person aus spezifischen Rechtsvorschriften abgeleitet werden. Insbesondere Artikel 53 Absatz 2 der

Strafprozessordnung[78] sieht vor, dass „personenbezogene Daten, die in Dokumenten über Prozesse und beschlagnahmte Gegenstände gespeichert sind“, vom Anwendungsbereich der individuellen Rechte in Kapitel IV des APPIHAO ausgenommen sind. Konkret geht der EDSA daher davon aus, dass betroffene Personen im Zusammenhang mit Strafverfahren nicht in den Genuss des Rechts auf Information, Auskunft, Berichtigung oder Löschung von personenbezogenen Daten kommen, die in Dokumenten zu Prozessen und beschlagnahmten Gegenständen gespeichert sind.

186. In Bezug auf diese Beschränkungen geht der EDSA davon aus, dass sie im Zusammenhang mit Daten, die auf der Grundlage von Anordnungen erhoben werden, sowie im Zusammenhang mit Daten, die im Wege der freiwilligen Offenlegung über Auskunftsformulare erhoben werden (siehe weiter unten), angewandt werden. Da die Rechtsgrundlage der beiden Verfahren für den Zugang zu den Daten (per Anordnung bzw. Auskunftsformular) in der Strafprozessordnung zu finden ist, findet Artikel 53-2 dieses Gesetzes offenbar auf beide Arten der Erhebung Anwendung. Da jedoch in Artikel 53-2 von „beschlagnahmten“ Gegenständen die Rede ist, könnte geklärt werden, ob die in dieser Bestimmung vorgesehenen Beschränkungen der Rechte auch im Rahmen der freiwilligen Offenlegung gelten.

187. Der EDSA bedauert, dass ihm nicht die Verordnungen der Präfekturpolizei vorliegen, von denen es heißt, dass sie in gleichem Maße wie das APPIHAO personenbezogene Daten, Rechte und Pflichten schützen. Angesichts der fehlenden Klarheit in Bezug auf die Auslegung des APPIHAO sowie der Tatsache, dass die Verordnungen der Präfekturpolizei nicht verfügbar sind, fragt sich der EDSA, ob die in diesem Zusammenhang den Betroffenen gewährten Rechte und die zusätzlichen Aufsichts- und/oder Rechtsschutzmechanismen ausreichen, um das Fehlen von Rechten zu kompensieren.

4.1.3.2 Rechtsbehelf durch unabhängige Behörden

4.1.3.2.1 Behördlicher Rechtsbehelf

188. Der EDSA stellt fest, dass Daten erhebende Verwaltungsorgane wie die Präfekturpolizei für die Bearbeitung von Anfragen von Einzelpersonen zu ihren – begrenzten – Rechten in Bezug auf ihre im Rahmen strafrechtlicher Ermittlungen erhobenen Daten zuständig sind (siehe weiter oben zu den verfügbaren Rechten), was offenbar die Erhebung von Daten auf der Grundlage sowohl einer Anordnung als auch von Auskunftsformularen umfasst. Konkret scheinen sich diese Rechte auf allgemeine Grundsätze zu beschränken, wie etwa die Notwendigkeit der Speicherung von Daten im Zusammenhang mit dem Zweck (siehe Artikel 3.1 APPIHAO), den Grundsatz der Zweckbindung (Artikel 4) oder die Richtigkeit der Daten (Artikel 5), während Rechte des Einzelnen wie das Recht auf Information, Auskunft, Berichtigung oder Löschung für personenbezogene Daten ausgeschlossen sind, die in Dokumenten über Prozesse und beschlagnahmten Gegenständen gespeichert sind.[79] Obwohl diese Organe nicht als unabhängig und damit als unabhängigen Rechtsbehelf oder unabhängige Aufsicht bietend angesehen werden können, begrüßt der EDSA diese Möglichkeit. Er betont jedoch, dass vor diesem Hintergrund eingereichte Beschwerden angesichts der im APPIHAO vorgesehenen Einschränkungen der Rechte auf sehr wenige Rechte der betroffenen Person beschränkt bleiben.

189. Da ferner „personenbezogene Daten, die in Dokumenten über Prozesse und in beschlagnahmten Gegenständen erfasst sind“, gemäß Artikel 53-2 der Strafprozessordnung vom Anwendungsbereich der individuellen Rechte in Kapitel IV des APPIHAO ausgeschlossen sind, ist die Möglichkeit, Auskunft über personenbezogene Daten zu beantragen, auch auf die Verfahren beschränkt, die in anderen

[78] Abrufbar unter http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 und zitiert in Anhang II des Entwurf des Angemessenheitsbeschlusses, Fußnote 25.

[79] Siehe weiter oben die Ausführungen zu den Einschränkungen im APPIHAO, und siehe insbesondere Artikel 53-2 der Strafprozessordnung (nicht vorgelegt, aber zitiert in Anhang II des Entwurfs des Angemessenheitsbeschlusses, Fußnote 25).

Bestimmungen der Strafprozessordnung vorgesehen sind. Anscheinend können nur Opfer, Verdächtige oder Beschuldigte in diesem Zusammenhang tätig werden, und dies nur je nach der Stufe des Strafverfahrens. Der EDSA macht sich daher Sorgen, dass betroffenen Personen nach japanischem Recht im Rahmen des Strafverfahrens kein allgemeines Recht auf Auskunft über Daten und/oder deren Berichtigung oder Löschung gewährt wird und dass alle verfügbaren Rechtsbehelfe implizieren, dass die Person entweder Opfer oder Verdächtiger oder Beschuldigter sein muss, oder dass ein Schaden nachgewiesen werden muss, doch sollten betroffene Personen auch das Recht haben, Auskunft über ihre Daten zu erhalten und ihre Daten berichtigen oder löschen zu lassen, wenn sie (evtl. noch) keinen Schaden erlitten haben und/oder wenn sie weder Opfer noch Verdächtiger oder Beschuldigter sind, sondern beispielsweise Zeuge.

4.1.3.2.2 Behördlicher Rechtsschutz durch die Präfekturkommission für öffentliche Sicherheit

190. Die Präfekturkommissionen für öffentliche Sicherheit scheinen ferner für die Bearbeitung von Beschwerden zuständig zu sein. Auf der Grundlage von Artikel 79 des im Entwurf des Angemessenheitsbeschlusses genannten Polizeigesetzes kann jede Person gegen ein rechtswidriges oder unangemessenes Verhalten eines Bediensteten bei der Wahrnehmung seiner Aufgaben Beschwerde einlegen.

191. Der EDSA strebt nach Klarheit in der Frage, ob eine „rechtswidrige" Verarbeitung personenbezogener Daten als „rechtswidriges oder unangemessenes Verhalten eines Bediensteten" gilt, und wie es um den Nachweis eines Nachteils steht, der offenbar von der betroffenen Person verlangt wird. In der Mitteilung der NPA an die Polizei und die Präfekturkommissionen für öffentliche Sicherheit bezüglich der ordnungsgemäßen Bearbeitung von Beschwerden im Zusammenhang mit der Wahrnehmung von Aufgaben durch Polizeibeamte sind die Beschwerden auf konkrete Forderungen im Zusammenhang mit der „Korrektur wegen besonderer Nachteile, die ein Polizeibeamter in Ausübung seiner Pflichten durch ein rechtswidriges oder unangemessenes Verhalten oder die Unterlassung der erforderlichen Maßnahmen verursacht hat" und die Möglichkeit der „Beschwerde/Unzufriedenheit über die unangemessene Ausführung der Amtshandlungen eines Polizeibeamten" beschränkt. Es wird ausdrücklich klargestellt, dass „Beschwerden wegen Nichterfüllung der Pflichten eines Polizeibeamten in Angelegenheiten, bei denen davon auszugehen ist, dass sie nicht in den Aufgabenbereich eines Polizeibeamten fallen, sowie Beschwerden, die eine allgemeine Meinung oder einen Vorschlag enthalten, der sich nicht unmittelbar auf die Beschwerde führende Partei selbst auswirkt, ausgeschlossen sind".

192. Bezüglich der Verfahrensvorschriften für die Einreichung einer Beschwerde stellt der EDSA fest, dass die Beschwerde zwar schriftlich eingereicht werden muss, dass aber bei ihrer Abfassung nach japanischem Recht Hilfestellung angeboten wird, und zwar auch für Ausländer. Darüber hinaus scheint die japanische Regierung die PPC auch mit der Aufgabe betraut zu haben, betroffene Personen in der EU bei der Bearbeitung und Klärung von Beschwerden in diesem Bereich zu unterstützen, was der EDSA begrüßt. Der EDSA betont, dass seinem Verständnis nach die PPC in diesem Zusammenhang nur als Kontaktstelle zwischen betroffenen Personen in der EU und den zuständigen Behörden in Japan fungieren wird.

193. Die Ergebnisse der Bearbeitung von Beschwerden durch die Präfekturkommission für öffentliche Sicherheit werden in den in Artikel 79-2 des Polizeigesetzes aufgeführten Fällen nicht mitgeteilt; dazu gehören auch Fälle, in denen der derzeitige „Wohnsitz des Beschwerdeführers unbekannt ist". Der EDSA erkennt an, dass die Bezugnahme auf den Wohnsitz nicht bedeutet, dass in allen Fällen betroffene Personen aus der EU von der Mitteilung der Ergebnisse ihrer Beschwerden aufgrund der Tatsache ausgeschlossen würden, dass sie ihren Wohnsitz nicht in Japan haben.

4.1.3.2.3 Ad-hoc-Verfahren unter Einbeziehung der PPC

194. In Anbetracht der oben beschriebenen Ergebnisse begrüßt der EDSA, dass die japanische Regierung und die EU-Kommission ein zusätzliches Rechtsschutzverfahren vereinbart haben, mit dem EU-Bürgern ein zusätzlicher Rechtsbehelf in Japan zur Verfügung gestellt wird, über den Privatpersonen auch gegen rechtswidrige oder nicht ordnungsgemäße Ermittlungen durch Behörden vorgehen können. Der EDSA stellt ebenfalls fest und begrüßt, dass die Anträge bei der PPC und nicht bei einer anderen Regierungsstelle gestellt werden können, wodurch der Zuständigkeitsbereich der PPC auf den Bereich der Strafverfolgung und der nationalen Sicherheit ausgeweitet wird.

195. Bei seiner Analyse des neuen Verfahrens hat sich der EDSA schwerpunktmäßig um ein Verständnis der Befugnisse der PCC in diesem Zusammenhang bemüht.

196. Auch wenn es sprachlich nicht ganz klar wird, geht der EDSA davon aus, dass das zusätzliche Rechtsschutzverfahren keine „Klagebefugnis“ in dem Sinne erfordert, dass der Antragsteller nicht nachweisen muss, dass seine personenbezogenen Daten wahrscheinlich einer Überwachung durch eine japanische Behörde unterzogen wurden. Der EDSA hätte noch immer gerne hierzu eine Bestätigung durch die Kommission.

197. Im Einklang mit seiner Bewertung des Ombudsperson-Verfahrens im Zusammenhang mit den Datenschutzschild betont der EDSA die Notwendigkeit wirksamer Befugnisse des Adressaten des Ersuchens, in diesem Fall der PPC, damit der Rechtsschutzmechanismus als mit einem wirksamen Rechtsbehelf im Sinne von Artikel 47 der Charta der Grundrechte im Wesentlichen gleichwertig betrachtet werden kann.

198. Bei der Erläuterung des Rechtsschutzmechanismus verweist die japanische Regierung auf die Artikel 6, 61 Ziffer ii und 80 APPI und stellt diese Befugnisse in Anhang II dar. Der EDSA geht davon aus, dass das in Anhang II beschriebene Verfahren die Befugnisse der PPC spezifiziert oder erweitert, da die Formulierungen in Artikel 6, 61 Ziffer ii und 80 APPI recht vage und allgemein sind. Soweit Anhang II die Befugnisse der PPC spezifiziert oder erweitert, bittet der EDSA um eine Klarstellung dazu, ob die anderen Agenturen der japanischen Regierung an sie gebunden sind.

199. Auf der Grundlage des Verfahrens in Anhang II stellt der EDSA fest, dass die zuständigen Behörden in Japan verpflichtet sind, mit der PPC zusammenzuarbeiten, „indem sie unter anderem ihr die erforderlichen Informationen und sachdienlichen Unterlagen zur Verfügung stellen, damit die PPC prüfen kann, ob die Erhebung oder die anschließende Verwendung personenbezogener Daten im Einklang mit den geltenden Bestimmungen erfolgt ist“. Für eine Beurteilung der Wirksamkeit des Systems ist es daher wichtig, erneut auf die Befugnisse dieser zuständigen Behörden hinzuweisen, mit denen die PPC zusammenarbeitet. Der EDSA geht davon aus, dass diese Befugnisse durch die Zusicherungen in Anhang II nicht erweitert würden.

200. Der EDSA stellt ferner fest, dass bei einem erwiesenen Verstoß gegen die Vorschriften „die Zusammenarbeit der betreffenden Behörden mit der PPC die Verpflichtung einschließt, gegen den Verstoß vorzugehen“, was ausdrücklich die Löschung der unter Verstoß gegen die geltenden Vorschriften erhobenen Daten umfasst. Der EDSA geht davon aus, dass die Verpflichtungen der zuständigen Behörde von der „Zusammenarbeit mit der PPC“ und nicht von einer Entscheidung der PPC herrühren.

201. Abschließend unterrichtet die PPC den Antragsteller über das „Ergebnis der Prüfung sowie über gegebenenfalls ergriffene Abhilfemaßnahmen“. Außerdem informiert die PPC den Antragsteller über die „Möglichkeit, eine Bestätigung des Ergebnisses bei der zuständigen Behörde einzuholen, und über die Behörde, an die ein solches Ersuchen um Bestätigung zu richten ist“.

202. Darüber hinaus hat die PPC zugesagt, den Antragsteller bei weiteren Maßnahmen nach japanischem Recht zu unterstützen, wenn der Antragsteller mit dem Ergebnis des Verfahrens nicht zufrieden ist.

203. Angesichts der Notwendigkeit, einen wirksamen Rechtsschutzmechanismus zu haben, der im Wesentlichen den EU-Standards gleichwertig ist, fragt sich der EDSA jedoch, ob die PPC über die Bewertung der Frage, ob die Erhebung oder die anschließende Nutzung personenbezogener Daten im Einklang mit den geltenden Vorschriften erfolgt ist, und über die Aufforderung der zuständigen Behörden, ihre jeweiligen Befugnisse zu nutzen und sich mit Beschwerden zu befassen, die ihnen von der PPC übermittelt werden, hinausgehende spezifische Befugnisse hat. Sollte die PPC nur als Ansprechpartner für die EU-Bürger fungieren, würde der EDSA dies als nicht ausreichend für einen wirksamen Rechtsschutzmechanismus betrachten, der im Wesentlichen den EU-Standards gleichwertig ist. Der EDSA fordert die Kommission daher auf, nähere Erläuterungen zu den in diesem Unterkapitel erwähnten Punkten zu liefern, insbesondere zu der Frage, ob und wie der Mechanismus die Verpflichtungen der zuständigen Behörden erweitert, inwieweit sie daran gebunden sind und wie die PPC wirksam die Einhaltung der Vorschriften gewährleisten und nicht nur als Anlaufstelle für EU-Bürger fungieren kann.

4.1.3.3 Gerichtliche Rechtsbehelfe

4.1.3.3.1 Quasi-Beschwerdeverfahren

204. Das so genannte „Quasi-Beschwerdeverfahren“ ermöglicht es, gegen die obligatorische Erhebung von Informationen aufgrund einer Anordnung vorzugehen, damit eine rechtswidrige Beschlagnahme aufgehoben oder abgeändert werden kann.

205. Dieser Weg setzt voraus, dass sich die Person der Tatsache bewusst ist, dass die Daten beschlagnahmt wurden. Der EDSA geht jedoch davon aus, dass das Verfahren für die Erhebung von Daten auf der Grundlage einer Anordnung der betroffenen Person nicht mitgeteilt wird. Ferner geht er davon aus, dass freiwillige Offenlegung nicht bedeutet, dass die angefragten Unternehmen verpflichtet sind, die betroffenen Personen über eingegangene Anfragen und deren Erledigung zu unterrichten. Obwohl in Anhang II betont wird, dass „eine solche Anfechtung erfolgen kann, ohne dass die Person den Abschluss des Falls abwarten muss“, ist in der Praxis, abgesehen von Anordnungen zur Genehmigung von Abhörmaßnahmen, bei denen im Gesetz eine Unterrichtungspflicht vorgesehen ist[80], dieser Weg anscheinend nur wirksam verfügbar, wenn die betroffene Person durch eine gegen sie angestrengte Rechtssache von der Erhebung Kenntnis erlangt hat.

4.1.3.3.2 Einstweilige Verfügung

206. Um die Löschung von Daten zu erwirken, die im Rahmen eines Strafverfahrens erhoben wurden (die so genannte „einstweilige Verfügung“), oder um Schadenersatz zu erhalten, können Einzelpersonen auch Zivilklage einreichen.

207. Im Hinblick auf Schadenersatz stellt der EDSA fest, dass das Verfahren auf Situationen beschränkt zu sein scheint, in denen ein Amtsträger in Ausübung seines Amtes rechtswidrig und fehlerhaft (vorsätzlich oder fahrlässig) der betroffenen Person Schaden zugefügt hat. Nach dem Verständnis des EDSA scheint der Schaden auch immaterielle Schäden zu umfassen. Es wird jedoch nicht näher ausgeführt, welche Nachweise die Person für einen erlittenen Schaden vorzulegen hat. Der EDSA war nicht in der Lage, die Rechtsprechung in Bezug auf die Gewährung von Schadenersatz zu bewerten,

[80] Artikel 23 des Gesetzes über das Abhören des Telefonverkehrs wird zwar auf S. 33 des Entwurfs des Angemessenheitsbeschlusses erwähnt, doch lag dem EDSA dieser Text nicht vor, weshalb er nicht beurteilen kann, in welchem Umfang diese Unterrichtungspflicht gilt und in welchen Fällen sie eingeschränkt sein könnte.

und kann daher nicht einschätzen, ob dieser Weg einen wirksamen Rechtsbehelf im Falle eines Schadens darstellt.

208. In Bezug auf die „einstweilige Verfügung“ hält der EDSA ferner fest, dass eine Person, bevor sie einen Antrag stellen kann, zunächst wissen sollte, dass ihre Daten erhoben wurden und weiterhin gespeichert werden. Angesichts der begrenzten Informations- und Auskunftsrechte von Personen im Zusammenhang mit strafrechtlichen Ermittlungen und Verfahren dürfte die Effizienz des Verfahrens daher eher begrenzt sein.

4.1.3.4 Allgemeine Bewertung der Möglichkeiten zur Einlegung von Rechtsmitteln

209. Nach Prüfung aller Rechtsbehelfsmöglichkeiten, die Einzelpersonen nach japanischem Recht sowie betroffenen Personen in der EU vor der PPC offenstehen, begrüßt der EDSA den *Ad hoc*-Streitbeilegungsmechanismus, in den die PPC einbezogen ist. Er bietet einen Mehrwert für betroffene Personen in der EU, weil er ihnen insbesondere aufzeigt, welche Wege ihnen zur Verfügung stehen, um Rechtsbehelfe und/oder Entschädigungen zu erhalten, und wie sie ihre Anträge gemäß den geltenden Verfahrensanforderungen nach japanischem Recht einzureichen haben. Es sind jedoch weitere Klarstellungen erforderlich, insbesondere zu der Frage, ob und wie der Mechanismus die Verpflichtungen der zuständigen Behörden ausweitet, inwieweit sie daran gebunden sind und wie die PPC wirksam die Einhaltung der Vorschriften sicherstellen kann, um zu gewährleisten, dass dieser neue Mechanismus einen wirksamen Rechtsbehelf bietet.

210. Diese Prüfung zeigt, dass offensichtlich kein Rechtsschutzmechanismus im japanischen Recht Auskunft über Daten bzw. deren Berichtigung oder Löschung für betroffene Personen vorsieht, die nicht Opfer, Verdächtige oder Beschuldigte im Zusammenhang mit einem Strafverfahren sind, um z. B. die rechtswidrige Erhebung oder Speicherung ihrer Daten zu korrigieren. Ferner hat sie ergeben, dass alle nach japanischem Recht für Opfer, Verdächtige oder Beschuldigte zur Verfügung stehenden Rechtsbehelfs- und Schadenersatzmechanismen implizieren, dass die Erhebung der Daten bekannt ist, was aber in der Praxis eher selten der Fall ist, da ihnen nur eingeschränkt Auskunft und Informationen erteilt werden. Darüber hinaus besteht weiterer Klärungsbedarf hinsichtlich des Nachweises eines rechtswidrigen Verhaltens seitens der Behörden, insbesondere in Bezug auf die Frage, ob ein solches Verhalten eine rechtswidrige Verarbeitung personenbezogener Daten beinhaltet, oder des Nachweises eines der Person entstandenen Schadens.

211. Sofern ihm keine weiteren Informationen und Anhaltspunkte vorgelegt werden, hegt der EDSA daher Bedenken, ob die im japanischen Recht und im Entwurf des Angemessenheitsbeschlusses genannten Rechtsbehelfe im Vergleich zu den Standards des EU-Rechts hinreichend wirksam sind.

4.2 Zugang für Zwecke der nationalen Sicherheit

4.2.1 Umfang der Überwachung

212. Im Entwurf des Angemessenheitsbeschlusses wird das Kapitel über den „Zugang japanischer Behörden zu Daten für Zwecke der nationalen Sicherheit und deren Nutzung durch die japanischen Behörden“ im Einklang mit der von der japanischen Regierung in Anhang II gemachten Zusicherung eingeführt, nach der kein japanisches Gesetz „obligatorische Informationsersuchen“ oder „das Abhören des Telefonverkehrs zu administrativen Zwecken“ außerhalb von strafrechtlichen Ermittlungen zulassen würde. Abschließend heißt es, dass „aus Gründen der nationalen Sicherheit Informationen nur aus einer Quelle gewonnen werden dürfen, die für jedermann oder durch freiwillige Offenlegung frei zugänglich ist. Dies schließt verdeckte Überwachungstätigkeiten in diesem Bereich aus. Unternehmer,

die eine Anfrage nach freiwilliger Zusammenarbeit (in Form der Offenlegung elektronischer Informationen) erhalten, sind rechtlich nicht verpflichtet, derartige Informationen bereitzustellen".[81]

213. Innerhalb dieser Grenzen sind vier staatliche Stellen aufgeführt, die befugt sind, aus Gründen der nationalen Sicherheit im Besitz japanischer Unternehmen befindliche elektronische Daten zu erheben. Zum Verteidigungsministerium, einer dieser vier Stellen, heißt es, dass es „nur befugt [ist], (elektronische) Informationen durch freiwillige Offenlegungen zu erheben".[82]

214. Zur Bewertung der allgemeinen Gestaltung der Datenerhebung für Zwecke der nationalen Sicherheit möchte der EDSA an die erste der vier so genannten „wesentlichen Garantien" erinnern, wonach die „Verarbeitung auf klaren, präzisen und zugänglichen Vorschriften beruhen sollte".[83] Der EGMR hat hierzu ganz ausdrücklich festgestellt, dass Überwachungsprogramme nur dann „im Einklang mit dem Gesetz" stehen, wenn die Überwachungsmaßnahmen „eine gewisse Grundlage im innerstaatlichen Recht haben". Der Gerichtshof hat klargestellt, dass die Vereinbarkeit mit dem Rechtsstaatsprinzip verlangt, dass das Gesetz, mit dem die Maßnahme genehmigt wird, zugänglich und in seinen Wirkungen vorhersehbar sein muss. Unter Hinweis auf das Willkürrisiko hat der Gerichtshof „klare und detaillierte Vorschriften für geheime Überwachungsmaßnahmen" verlangt, die „hinreichend klar sind, damit die Bürger einen angemessenen Hinweis auf die Umstände und Bedingungen erhalten, unter denen Behörden befugt sind, solche Maßnahmen zu erlassen".[84]

215. Mit Blick auf die Anwendung dieser wesentlichen Garantien auf das japanische Rechtssystem ist sich der EDSA nicht nur der Tatsache bewusst, dass die Staaten in Angelegenheiten der nationalen Sicherheit über einen großen Ermessensspielraum verfügen, der vom Europäischen Gerichtshof für Menschenrechte anerkannt wird. Die Befugnisse im Bereich der nationalen Sicherheit spiegeln auch die historischen Erfahrungen der Nationen wider. Der EDSA geht daher davon aus, dass, wie von der japanischen Regierung betont, nach dem Zweiten Weltkrieg die Befugnisse der nationalen Nachrichtendienste in Japan deutlicher eingeschränkt wurden als in anderen Staaten.

216. Aus Sichtweise des EDSA legt der Entwurf des Angemessenheitsbeschlusses im Einklang mit der Zusicherung der japanischen Regierung nahe, dass japanische Regierungsstellen keine Programme betreiben, die eine strategische Überwachung oder eine breit angelegte Überwachung von Kommunikation (Internet) bedeuten. Wie bereits ausgeführt, hat die japanische Regierung in einem vom Justizminister unterzeichneten Schreiben zugesichert, dass „aus Gründen der nationalen Sicherheit Informationen nur aus einer Quelle gewonnen werden dürfen, die für jedermann oder durch freiwillige Offenlegung frei zugänglich ist".

217. Bezüglich der Rechtsgrundlage des Verteidigungsministeriums stellt der EDSA fest, dass der Entwurf eines Angemessenheitsbeschlusses allgemeine Informationen über seine Befugnisse enthält und zu seinen Aufgaben zählt, „solche Angelegenheiten so zu handhaben, dass der nationale Friede und die Unabhängigkeit sowie die Sicherheit der Nation gewahrt sind". Dem EDSA liegt jedoch keine englische Übersetzung dieser Rechtsgrundlage vor.

218. Der EDSA hat aber auch Kenntnis von verschiedenen Medienberichten, in denen es heißt, dass von der Direktion für Signalaufklärung im japanischen Verteidigungsministerium Überwachungsprogramme

[81] Angemessenheitsbeschluss, Ziffer 151.
[82] Angemessenheitsbeschluss, Ziffer 153.
[83] Artikel 29-Datenschutzgruppe, WP237: Arbeitsunterlage 01/2016 über die Rechtfertigung von Eingriffen in die Grundrechte auf Schutz der Privatsphäre und Datenschutz durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten (Wesentliche europäische Garantien).
[84] Siehe z. B. Big Brother Watch und andere / Vereinigtes Königreich, Rn. 305.

durchgeführt werden.[85] In dem Bericht wird auch behauptet, das japanische Verteidigungsministerium habe sich zwar geweigert, die Einzelheiten des Berichts zu erörtern, habe aber eingeräumt, Japan habe „Büros im ganzen Land“, die Kommunikation abhören, und diese konzentrierten sich „auf militärische Aktivitäten und Cyberbedrohungen“ und erhöben „keine Daten über die breite Öffentlichkeit“. Letztere Erklärung (dass das Verteidigungsministerium keine Informationen über die breite Öffentlichkeit sammelt) wird von der japanischen Regierung zum Teil der Bekräftigung gemacht.

219. Die japanische Regierung hat in einem vom Justizminister unterzeichneten Schreiben erneut bekräftigt, dass das Verteidigungsministerium keine Informationen über die breite Öffentlichkeit sammelt.

220. Eine allgemeine Beurteilung der möglichen Überwachungsfähigkeiten der japanischen Regierung geht über die Aufgabe des EDSA hinaus. Diese Tätigkeiten sind für seine Bewertung nur dann von Belang, wenn sie für die Übermittlung personenbezogener Daten zwischen der EU und Japan relevant sind. In diesem Zusammenhang möchte sich der EDSA der von seinem Vorgängergremium im Zusammenhang mit einer Stellungnahme zu EU-US-Datenschutzschild beschlossenen Vorgehensweise anschließen. In ihrer Stellungnahme zum Datenschutzschild ist die Artikel 29-Datenschutzgruppe in ihrer Analyse auf die Befugnisse und Grenzen für die USA bei der Überwachung von Daten „auf ihrem Weg“ in die USA eingegangen.[86] Wendet man den gleichen Standard auf den Angemessenheitsbeschluss zu Japan an, sind nach Auffassung des EDSA Informationen über die Befugnisse der japanischen Behörden, die Daten „auf ihrem Weg“ nach Japan zu überwachen, von Belang. Sollten diese Überwachungsbefugnisse gegeben sein, scheint auch die Entscheidung des EGMR in *Big Brother Watch* darauf hinzudeuten, dass diese Befugnisse im Einklang mit den durch die EMRK festgelegten Normen geregelt werden müssten.

221. Sollten Überwachungsmaßnahmen auf die „Unterstützung militärischer Maßnahmen“ beschränkt sein, könnte es sein, dass sie für die Beurteilung des Angemessenheitsbeschlusses nicht relevant sind. Es liegt daher im Interesse des EDSA, Klarstellungen zu den Überwachungsmaßnahmen der japanischen Regierungsstellen zu erhalten. In diesem Zusammenhang wäre eine solche Klarstellung zur Beantwortung der Frage wünschenswert, ob Daten, die vor dem Hintergrund dieses Angemessenheitsrahmens übermittelt werden, für Zwecke der nationalen Sicherheit von den in diesem Bereich zuständigen japanischen Behörden abgerufen werden können.

4.2.2 Freiwillige Offenlegung im Zusammenhang mit nationaler Sicherheit

222. Im Entwurf des Angemessenheitsbeschlusses heißt es, dass die vier staatlichen Stellen nur befugt sind, (elektronische) Informationen durch freiwillige Offenlegung zu erheben. Gemäß dem Beschlussentwurf und Anhang II gibt es einige Beschränkungen aus gesetzlichen Gründen, was bedeutet, dass die Datenerhebung auf das beschränkt ist, was für die Stellen zur Wahrnehmung ihrer Aufgaben erforderlich ist.

[85] Im Mai 2018 veröffentlichte die Online-Publikation „The Intercept“ einen Bericht mit dem Titel „The untold story of Japan’s secret spy agency“ (Die unbekannte Geschichte der geheimen Spionageagentur Japans).

[86] Siehe WP255, EU-US-Datenschutzschild – Erste jährliche gemeinsame Überprüfung, angenommen am 28. November 2017, S. 16: „Die Artikel 29-Datenschutzgruppe ist der Ansicht, dass die Analyse der Rechtsvorschriften des Drittlandes, dessen Angemessenheit geprüft wird, nicht auf die Rechtsvorschriften und Praktiken beschränkt sein sollte, die eine Überwachung innerhalb der physischen Grenzen dieses Landes ermöglichen, sondern auch eine Analyse der rechtlichen Voraussetzungen in dem Recht dieses Drittlandes enthalten sollte, die es in die Lage versetzen, außerhalb seines Hoheitsgebiets im Hinblick auf EU-Daten Überwachung vorzunehmen. Wie bereits in ihrer früheren Stellungnahme betont wurde, „sollte klar sein, dass die Grundsätze des Datenschutzschilds ab dem Zeitpunkt gelten, zu dem die Datenübermittlung stattfindet, d. h. auch in Bezug auf die Daten „auf ihrem Weg“ in dieses Land“.

223. Wie schon im Abschnitt über Strafverfolgung erwähnt, ist im Bereich des Strafrechts die freiwillige Offenlegung nur im Rahmen einer strafrechtlichen Ermittlung zulässig und setzt somit einen konkreten Verdacht auf eine bereits begangene Straftat voraus. Untersuchungen im Bereich der nationalen Sicherheit unterscheiden sich von Ermittlungen im Bereich der Strafverfolgung. Der EDSA erkennt an, dass gemäß Anhang II die zentralen Grundsätze der „Notwendigkeit der Untersuchung" und der „Angemessenheit der Methode" sinngemäß auch für den Bereich der nationalen Sicherheit gelten und unter Berücksichtigung der besonderen Umstände des jeweiligen Falls gewahrt werden müssen.[87] Er bedauert, dass die Anwendung nicht weiter präzisiert wird, auch nicht durch einen Verweis auf die Rechtsprechung. Allerdings hält der EDSA fest, dass die Anwendung dieses Verfahrens verhältnismäßig oder notwendig sein muss.

224. Wurden personenbezogene Daten erhoben („erlangt"), ist gemäß dem Entwurf des Beschlusses ihre Verarbeitung im APPIHAO (mit Ausnahme der Präfekturpolizei) geregelt.[88] In Anhang II heißt es, dass die Verarbeitung personenbezogener Daten durch die Präfekturpolizei durch Verordnungen des Präfekten geregelt wird, in denen Grundsätze für den Schutz personenbezogener Daten sowie Rechte und Pflichten festgelegt sind, die denen des APPIHAO gleichwertig sind.[89] Da für diese Verordnungen keine englischen Übersetzungen vorliegen, kann der EDSA nicht beurteilen, ob die Grundsätze denen des APPIHAO gleichwertig sind.

225. Für weitere Anmerkungen zur freiwilligen Offenlegung wird auf den Abschnitt über Strafverfolgung verwiesen.

4.2.3 Aufsicht

4.2.3.1 Allgemeine Anmerkungen

226. Die folgenden vier staatlichen Stellen sind befugt, aus Gründen der nationalen Sicherheit elektronische Informationen im Besitz von japanischen Unternehmern zu erheben: i) das Cabinet Intelligence & Research Office (CIRO); ii) das Verteidigungsministerium (MOD); iii) die Polizei (sowohl die Nationale Polizeibehörde (NPA)[90] als auch die Präfekturpolizei) und iv) der Geheimdienst Public Security Intelligence Agency (PSIA).

227. Gemäß dem Entwurf des Angemessenheitsbeschlusses unterliegen diese staatlichen Stellen mehreren Ebenen der Aufsicht seitens der drei Gewalten.[91] Der EDSA stellt fest, dass es einen Aufsichtsmechanismus innerhalb der Legislative (japanisches Parlament) und die Exekutive (Büro für Rechtskonformität (IGO) der Generalinspektion, die Präfektur-Kommissionen für öffentliche Sicherheit und die Kommission für die Prüfung der öffentlichen Sicherheit) gibt. Der EDSA unterstreicht, dass die Kommission Präzisierungen zur gerichtlichen Kontrolle (*ex officio* / Garantie C aus WP 237); für Rechtsbehelfe gibt es ein gesondertes Kapitel im Entwurf des Beschlusses und eine zusätzliche Garantie in WP 237) über die oben genannten staatlichen Stellen vorlegen sollte, da unklar ist, ob eine solche gerichtliche Kontrolle im Bereich der Erhebung personenbezogener Daten für Zwecke der nationalen Sicherheit ohne Zwangsmittel überhaupt besteht.

[87] Siehe Anhang II, S. 23.
[88] Angemessenheitsbeschluss, Ziffern 118 und 157.
[89] Siehe Anhang II, S. 3.
[90] Den vorliegenden Informationen zufolge besteht die Hauptaufgabe der NPA jedoch darin, die Ermittlungen der verschiedenen Präfektur-Polizeidienststellen zu koordinieren, und ihre Tätigkeiten im Bereich der Datenerhebung sind auf den Austausch mit ausländischen Behörden beschränkt.
[91] Siehe Anhang II, S. 39.

4.2.3.2 Aufsicht durch das japanische Parlament

228. Der EDSA hält fest, dass das japanische Parlament Untersuchungen in Bezug auf die Tätigkeiten von Behörden und somit auch von allen genannten staatlichen Stellen durchführen kann. Darüber hinaus kann das Parlament auch die Vorlage von Dokumenten und Zeugenaussagen verlangen (*Artikel 62 der japanischen Verfassung, Artikel 104 des Gesetzes über das Parlament*). Der EDSA hält ferner fest, dass gemäß *Artikel 74 und 75 des Gesetzes über das Parlament* Mitglieder des japanischen Parlaments schriftliche Anfragen an das Kabinett richten können, die das Kabinett beantworten kann (*Artikel 75 des Gesetzes über das Parlament*). Schließlich wird auch darauf hingewiesen, dass es spezifische Berichtspflichten, z. B. für die Public Security Intelligence Agency (PSIA) (Artikel 36 SAPA/Artikel 31 ACO), mit einem jährlichen Bericht an das Parlament gibt. Ein solcher Bericht lag dem EDSA jedoch nicht vor.

4.2.3.3 Aufsicht durch das Büro für Rechtskonformität (IGF) des Generalinspektors

229. Der EDSA stellt fest, dass es für das Verteidigungsministerium eine Aufsichtsstelle gibt, nämlich das so genannte IGO. Dem EDSA lag das Gesetz zur Einrichtung des Verteidigungsministeriums nicht vor, lediglich die Darstellungen in Anhang II des Beschlussentwurfs. Gemäß Anhang II ist das IGO ein unabhängiges Büro innerhalb des Verteidigungsministeriums, das gemäß Artikel 29 des Gesetzes zur Einrichtung des Verteidigungsministeriums unmittelbar dem Verteidigungsminister unterstellt ist. Das IGO ist befugt, die Einhaltung von Gesetzen und sonstigen Vorschriften durch Beamte des Verteidigungsministeriums (so genannte „Defense Inspections“) im gesamten Ministerium, einschließlich der Selbstverteidigungsstreitkräfte, zu überprüfen.

230. Gemäß Anhang II nimmt das IGO seine Aufgaben unabhängig von den operativen Dienststellen des Verteidigungsministeriums wahr. Der EDSA hält fest, dass das IGO ein *internes* Aufsichtsgremium ist.

231. Inspektionen führen zu Feststellungen und – um die Einhaltung der Vorschriften zu gewährleisten – Maßnahmen, die direkt dem Verteidigungsminister gemeldet werden. Auf der Grundlage des Berichts des IGO kann der Verteidigungsminister Weisung erteilen, die zur Abhilfe erforderlichen Maßnahmen zu ergreifen. Der stellvertretende Minister für Verteidigung ist für die Umsetzung dieser Maßnahmen verantwortlich und muss dem Verteidigungsminister über den Stand der Umsetzung Bericht erstatten.

232. Nach Analyse von Anhang II, ohne dass ihm jedoch die einschlägigen Rechtsvorschriften (Gesetz über die Einrichtung des Verteidigungsministeriums) vorlagen, begrüßt der EDSA die Möglichkeit, Anweisungen bezüglich der erforderlichen Maßnahmen zur Einhaltung der Vorschriften zu erteilen, um Abhilfe zu schaffen. Der EDSA äußert jedoch Zweifel an der Unabhängigkeit des IGO, da es sich gemäß Anhang II um ein Büro innerhalb des Verteidigungsministeriums handelt und es unmittelbar dem Verteidigungsminister unterstellt ist (hierzu heißt es in *WP 237*: *„(...) ist die funktionale Unabhängigkeit allein nicht ausreichend, um diese Aufsichtsbehörde vor jeglicher Einflussnahme von außen zu schützen*“).

233. Im Einklang mit der Rechtsprechung des EGMR und der Arbeitsunterlage *WP 237* bzw. aufgrund der Erwägungen in Anhang II kann der Generalinspekteur Berichte von der betreffenden Dienststelle anfordern (Dokumente, Websites, Erläuterungen). Es muss nach Auffassung des EDSA geklärt werden, ob die betreffenden Dienststellen verpflichtet sind, diesen Ersuchen nachzukommen und ob die angeforderten Dokumente auch Verschlusssachen umfassen, wie in *WP 237* erwähnt.

234. Auch wenn der EDSA begrüßt, dass wirklich hochrangige Rechtsexperten (ehemalige Leitende Staatsanwälte) das IGO leiten, erscheint eine Präzisierung hinsichtlich der Art und Weise notwendig, wie dieses Aufsichtsgremium besetzt wird.

4.2.3.4 Aufsicht durch die Kommission für die Prüfung der öffentlichen Sicherheit

235. Gemäß Anhang II (S. 25) führt PSIA regelmäßige und besondere Inspektionen der Tätigkeiten ihrer einzelnen Dienststellen und Büros durch (PSIA, Dienststellen und nachgeordnete Dienststellen der PSIA usw.). Für die Zwecke der regelmäßigen Kontrolle werden ein Assistent des Generaldirektors und/oder ein Direktor als Aufsichtsbeamte benannt. Diese Inspektionen sollten auch die Verwaltung personenbezogener Daten betreffen.

236. Gemäß Erwägungsgrund 163 des Beschlussentwurfs fungiert die Kommission für die *Prüfung der öffentlichen Sicherheit* als unabhängige Ex-ante-Aufsichtsbehörde für die PSIA im Hinblick auf Fragen von ACO[92] und SAPA[93]. Der EDSA begrüßt dies.

237. Auch wenn die Website des japanischen Justizministeriums einige Informationen enthält[94], ist der EDSA nicht in der Lage, die Unabhängigkeit der Kommission für die Prüfung der öffentlichen Sicherheit sorgfältig zu bewerten, da ihm weder der Rechtsakt zur Einrichtung der Kommission für die Prüfung der öffentlichen Sicherheit[95] noch die Geschäftsordnung der Kommission für die Prüfung der öffentlichen Sicherheit[96] vorlagen.

4.2.3.5 Aufsicht durch die Nationale Kommission für öffentliche Sicherheit, Präfekturkommissionen für öffentliche Sicherheit und das APPIHAO (Exekutive)

238. Siehe 3.1.2.2.1 (Nationale Kommission für öffentliche Sicherheit), 3.1.2.2.2. (Präfekturkommissionen für öffentliche Sicherheit) und 3.1.2.2.4. (Exekutive).

4.2.3.6 Aufsicht durch die PPC

239. Der EDSA fordert die Kommission auf, entweder in Erwägungsgrund 164 darauf hinzuweisen, dass die PPC kein Aufsichtsgremium für die oben genannten staatlichen Stellen und nur für den Rechtsschutz der Personen zuständig ist, oder die Passage in Erwägungsgrund 164 über die PPC in den Abschnitt „individueller Rechtsschutz“ zu verschieben.

4.2.4 Rechtsschutzmechanismus

240. Für die Analyse des neu ausgehandelten Rechtsschutzmechanismus wird auf den Abschnitt über Strafverfolgung verwiesen.

241. Darüber hinaus ist erwähnenswert, dass das japanische Recht eine spezielle individuelle Rechtsschutzmöglichkeit vorsieht, die im Bereich der nationalen Sicherheit zur Verfügung steht. Der EDSA geht davon aus, dass alle Einzelpersonen, auch EU-Bürger, generell die Offenlegung, Berichtigung (einschließlich Löschung) oder Aussetzung der Verwendung von Daten durch Verwaltungsorgane beantragen können, und zwar auch, wenn diese für Zwecke der nationalen Sicherheit verarbeitet werden. Wird ein solcher Antrag „abgelehnt mit der Begründung, dass die betreffenden Informationen als geheim zu betrachten sind“, kann eine Überprüfung beantragt werden und ist das „Information

[92] Gesetz über die Kontrolle von Organisationen, die Verbrechen des willkürlichen Massenmords begangen haben (Gesetz Nr. 147 vom 7. Dezember 1999).
[93] Gesetz Nr. 240 vom 21. Juli 1952 zur Verhütung subversiver Tätigkeiten.
[94] Siehe http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (September 2018): Das nicht zum Ministerium gehörende Gremium *„besteht aus einem Vorsitzenden und sechs Mitgliedern. Sie werden aus dem Kreis von Personen mit gutem Leumund ausgewählt, die in der Lage sind, ein faires Urteil über die Kontrolle von Organisationen und Personen mit umfassenden Kenntnissen und Erfahrungen sowohl des Rechts als auch der Gesellschaft abzugeben. Sie werden vom Premierminister ernannt und müssen von beiden Kammern des Parlaments gebilligt werden. In Bezug auf die Anwendung der zuvor genannten Gesetze (SAPA/ACO) nehmen die Mitglieder ihre Aufgaben recht unabhängig wahr und nehmen keine Weisungen des Ministerpräsidenten oder des Justizministers entgegen und unterstehen auch nicht deren Aufsicht.“*
[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (September 2018).
[96] Artikel 28 ACO.

Disclosure and Personal Information Protection Review Board“ zu konsultieren. Dieser Ausschuss setzt sich aus Mitgliedern zusammen, die vom Premierminister mit Zustimmung beider Kammern des Parlaments ernannt werden und mit Untersuchungsbefugnissen ausgestattet sind, und schließt seine Arbeiten mit einem schriftlichen Bericht für die betreffende Person ab, der nicht rechtsverbindlich ist, aber fast immer befolgt wird.[97] Gemäß Anhang II gab es nur zwei von 2 000 Fällen, in denen eine Verwaltungsbehörde eine Entscheidung erließ, die von der Schlussfolgerung des Ausschusses abwich.[98]

242. Aus der Erläuterung geht hervor, dass die Überprüfung nicht vorgenommen werden kann, wenn die Informationen „offengelegt“ werden können, der Einzelne jedoch mit dem Ergebnis nicht zufrieden ist. Der EDSA erkennt diese Möglichkeit für den Rechtsschutz an, hätte jedoch gerne weitere Erläuterungen zu letztgenanntem Aspekt, der deren Anwendungsbereich erheblich einschränken würde.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

[97] Siehe Anhang II, S. 25f. Gesetz zur Einrichtung des Überprüfungsausschusses für die Offenlegung von Informationen und für den Schutz personenbezogener Daten, Artikel 4, 9, 11.
[98] Anhang II Fußnote 35.